****

**High Level Design Template**

**Active Directory Consolidation**

***<Customer Logo>***

*<Project 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** |  |

*<Client Name>*

*Authors MSI EUS Directory Services Team. Final Review by Deepak A*

*<RFP Number>*

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

[1. Executive summary 6](#_Toc500634932)

[1.1. Purpose of the document 6](#_Toc500634933)

[1.2. In scope 6](#_Toc500634934)

[1.3. Out of scope 6](#_Toc500634935)

[2. Design Factors and scope 8](#_Toc500634936)

[2.1. Parameters are taken into consideration for AD consolidation 8](#_Toc500634937)

[2.2. Domain design factors 8](#_Toc500634938)

[2.3. Design Dependencies 8](#_Toc500634939)

[2.4. What impact will this solution have on implemented services? 8](#_Toc500634940)

[3. Assumptions, Issues and Risks 10](#_Toc500634941)

[3.1. Assumptions 10](#_Toc500634942)

[3.2. Issues 10](#_Toc500634943)

[3.3. Challenges 10](#_Toc500634944)

[3.4. Risks 11](#_Toc500634945)

[4. Architecture/Design Details & Procedures 12](#_Toc500634946)

[4.1. AD consolidation and migration framework 12](#_Toc500634947)

[4.2. Architecture/design of Active Directory consolidation 12](#_Toc500634948)

[4.2.1. Active Directory consolidation drivers 13](#_Toc500634949)

[4.2.2. Challenges of consolidating active directory 13](#_Toc500634950)

[4.2.3. Discovering and analyzing the source Active Directory environment 13](#_Toc500634951)

[4.2.4. Planning the target AD environment 13](#_Toc500634952)

[4.2.5. Identifying and remediating any applications that rely on the AD structure to ensure they will not cause business disruption during the migration 14](#_Toc500634953)

[4.2.6. Validating the new transition approach in a lab setting with AD migration tool (like Binary tree – AD migrator or Quest – QMM) 14](#_Toc500634954)

[4.2.7. Conducting a pilot project with a small number of users and resources, starting slowly and increasing velocity as the pilot achieve success 16](#_Toc500634955)

[4.2.8. Creating backup and recovery plans for unexpected issues that arise during the migration, allowing you to restore the previous AD environment without impacting users and organizational workflow 16](#_Toc500634956)

[4.2.9. Anticipating risks and establishing plans to address them 16](#_Toc500634957)

[4.2.10. Define the end state of active directory infrastructure 17](#_Toc500634958)

[4.2.11. Created a checklist for the active directory consolidation using AD migration tool 20](#_Toc500634959)

[4.2.12. Maintain active directory synchronization 25](#_Toc500634960)

[4.2.13. Maintain on going function and user functionality 26](#_Toc500634961)

[4.2.14. Migrate messaging or collaboration platforms 26](#_Toc500634962)

[4.2.15. Factors considered during migration of windows servers 26](#_Toc500634963)

[4.2.16. Roles & Responsibility 27](#_Toc500634964)

[4.2.17. Sign off 27](#_Toc500634965)

[4.2.18. Appendix 27](#_Toc500634966)

1. Executive summary
   1. Purpose of the document

This document describes an approach to active directory consolidation as followings:

* Intra-forests consolidation like consolidation of child domains into root domain in the forest.
* Inter-forests consolidation - consolidate active directory for corporate restructuring like merger, acquisition, devastation etc.
* Decommissions of child domain/forest in post active directory consolidation.

Active Directory consolidation methods includes but not limited to

* Active Directory consolidation drivers
* Challenges of consolidating active directory
* Best practices for Active directory consolidation by selection of active directory tool (like ADMT, Binary tree - AD migrator, Quest - QMM etc.). ADMT is not recommended for inter-forest migration.
* Define the end state of active directory infrastructure
* Created a checklist for the active directory consolidation
* Maintain active directory synchronization
* Maintain on going function and user functionality
* Migrate messaging or collaboration platforms
* Factors considered during migration of windows servers in conjunction with AD.
* Hyper care and Sign off
  1. In scope
* Approach to consolidate source and target active directory domain’s/forest’s due to merger, acquisition, devastation and evolution of active directory environment by reducing the environment complexity, management and maintenance cost etc.
* Decommissions of unwanted domains/forests in post AD consolidation.
  1. Out of scope

These areas are out of scope of this HLD:

* Changes to Active Directory to apply any other settings except ones mentioned in this document.
* Changes in the design of any other infrastructure services end-user devices depend upon.
* Changes in the design of end user devices.
* Application upgrades etc.

1. Design Factors and scope
   1. Parameters are taken into consideration for AD consolidation

* Single foundation
* Security
* Backup and recovery
* Hardware
* Faster deployment
  1. Domain design factors
* Geographical factors: Where organizations span may geographical regions, you might consider implementing a geographic domain design to control replication over different regions within the enterprise. Domain controllers would then only replicate data in its local domain.
* WAN link costs: The cost of implementing and maintaining unreliable WAN links could be high, as is the case in some countries.
* Business Requirement Factors: There may be cases where different businesses within the same organization can indeed share a forest, but the nature of their business might lead to each business needing to have its own domains. This is normally necessary when each business needs to implement its own domain security policies.
  1. Design Dependencies

Active directory consolidation deployment depends on:

* User based license for Active directory migration tool for Active Directory consolidation.
* RACI for Applications/servers from the application owner.
* Site wise assessment for planning and respective HW/virtual for new Domain Controllers in the target domain.
  1. What impact will this solution have on implemented services?

Proper migration checklist and RACI will be created in the planning phase before AD consolidation project.

* Absence of trust between source and target forest.
* Microsoft exchange is integrated with and relies upon active directory for key user and resource information. Any AD migration will impact user access to exchange mailboxes and have an impact on exchange migration.
* AD migration will frequently impact the SharePoint environment and will require modification of rights along with modification of user identities.
* Windows servers will be impacted for replacing of domain controllers, servers moved from one domain to another domain during AD consolidation.
* FIM, DNS, DHCP, ADFS, PKI, RAIUS, Centrify, DFS services and end user workstations will be impacted during AD consolidation.
* Some training might be required to help users to use Windows 10 and Office365. Pilot is recommended to assess what kind of support the business users might need.
  1. Roles & Responsibility (RACI Matrix)

<<SAMPLE>>

Following table represent the RACI matrix for AD consolidation project.

|  |  |  |
| --- | --- | --- |
| **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 functioal 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 the Target 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 Target domain after decommission of child domains (Hyper care period) | C,I | R,A |

1. Assumptions, Issues and Risks
   1. Assumptions

* “Approved AD migration tool” by the customer will be used to perform AD migration and security translation of servers.
* Required support/vendor will be engaged for application mitigation.
* Application owners will be providing the support during migration phase if needed;
* PoC, Pilot and Pre-Prod/Testing environments to test migration, applications etc. will be prepared to reduce a negative impact on the business
  1. Issues

Following known issues may be resolved by advance planning in the AD consolidation project:

* Setting up multiple trust between forests. Multiple trust path will not be established between forests.
* Accessing resource using Kerberos authentication using Alias (CNAME) in multiple domains. Conditional forwarder/Secondary zone will be used instead of CNAME.
* Same hostname exists in multiple domains. FQDN will be used to avoid this issue,
* Kerberos forest search order: SPN request made by the client as <HTTP://servername> instead of domain suffix.
* Cross forest usage of DFS namespace. DFSN will be updated to use DNS FQDN’s.
* Forgot to allow port 389 in firewall configuration for DC discovery operation.
* Partners vulnerability like health compliance between source and target forest will be exposed.
* Incompatible security policies like naming convention of GPO’s with settings between source and target forests.
  1. Challenges
* Absence of trust between source and target forest.
* Ability to migrate without shared admin access.
* AD is fully tie to the underlying network infrastructure.
* Need to update ACL’s all resources managed across the active directory environment between source and target.
  1. Risks

Risks’ likelihood of occurrence and impact are accessed on a scale from 1 to 3, where 1 – is low, 3 - high

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N** | **Risk** | **Likelihood of occurrence** | **Impact** | **Mitigation** |
| 1 | Application not stable in post AD consolidation project | 1 | 3 | Pilot test is recommended prior to production environment. |
| 2 | Engagement -Business Readiness: Lack of proper business change management | 1 | 1 | Business change management needs to be factored and planned as an integral part of the program |
| 3 | Improper GPO implementation: Wrong Linking of Group policies leads to security risks | 1 | 3 | Proper testing of GPO’s before moves to production |
| 4 | Network architecture may not be adequate to allow speedy deployment or provide all planned functionality | 1 | 2 | Ensure that network architecture is adequately prepared. For example, deploy QMM servers close to receiving workstations |
| 5 | Parallel projects: Dependent projects delays like exchange /SharePoint migrations | 1 | 2 | Need to coordinate with all dependent project owners |
| 6 | Non availability of Trust during migration | 1 | 3 | Ensure that network architecture is adequately prepared in both source and target environment. |
| 7 | Corrupted AD data in source domains | 1 | 3 | Regular backup and validation of NTDS.DIT |

1. Architecture/Design Details & Procedures
   1. AD consolidation and migration framework

Following diagram represents the AD consolidation and migration framework.

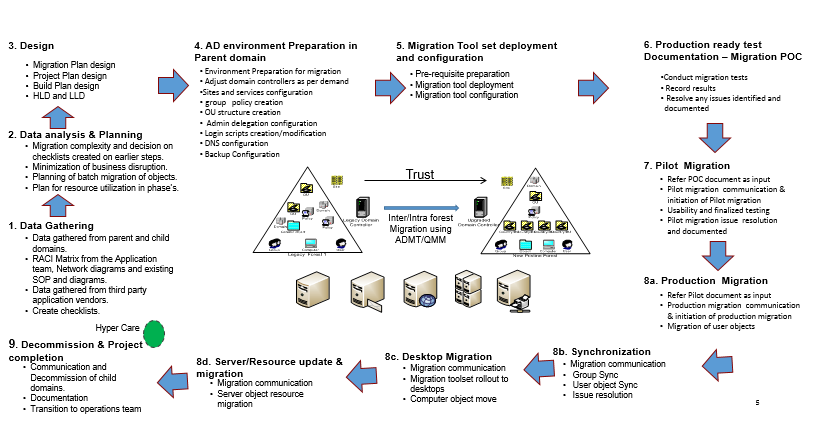


Figure - I

* 1. Architecture/design of Active Directory consolidation

Following diagram represents the flow of active directory consolidation.

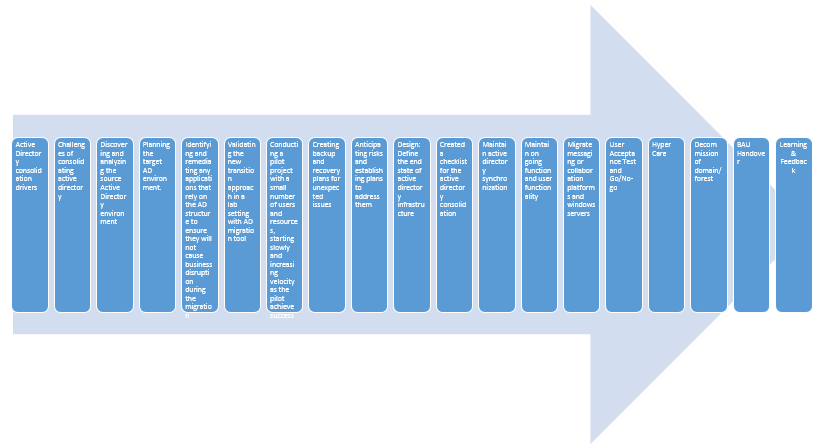


Figure – II

* + 1. Active Directory consolidation drivers
  1. Business driver: Corporate restructuring by merger and acquisition etc.
  2. Technical driver: Evolution of active directory environment by reducing the environment complexity, management and maintenance cost etc.
     1. Challenges of consolidating active directory
  3. Refer 3.3 section
     1. Discovering and analyzing the source Active Directory environment

**Input**

* Trust information of both the company’s
* DNS information of both the company’s
* Existing AD infrastructure of both the company’s
* Existing AD design documents- HLD/LLD
* Existing Application Inventories of both the company’s
* Number of sites/users of both the company’s
* Network topology of both the company’s

**Deliverables**

* High level project plan
* Application inventory dependent on AD
  + 1. Planning the target AD environment

**Input**

* Deliverables from Assessment phase
* Design guidelines
* Solution Outline

**Execution**

* Develop HLD and LLD
* Develop communication strategy
* Develop hardware & software procurement list

**Deliverables**

* Detailed project plan
* Communication and reporting protocols
* Test plans, Monitoring checklists
* Procurement plan

* + 1. Identifying and remediating any applications that rely on the AD structure to ensure they will not cause business disruption during the migration

|  |  |  |
| --- | --- | --- |
| **Affected Application** | **Impact (yes /no)** | **Remediation** |
| FIM |  |  |
| DNS |  |  |
| DHCP |  |  |
| ADFS |  |  |
| PKI |  |  |
| Proxy service – checkpoint |  |  |
| DFS |  |  |
| Centrify |  |  |
| O365 |  |  |
| Messaging |  |  |
| Enterprise Applications |  |  |
| Share Point |  |  |
| Local applications |  |  |

* + 1. Validating the new transition approach in a lab setting with AD migration tool (like Binary tree – AD migrator or Quest – QMM)

Migration flow of QMM:

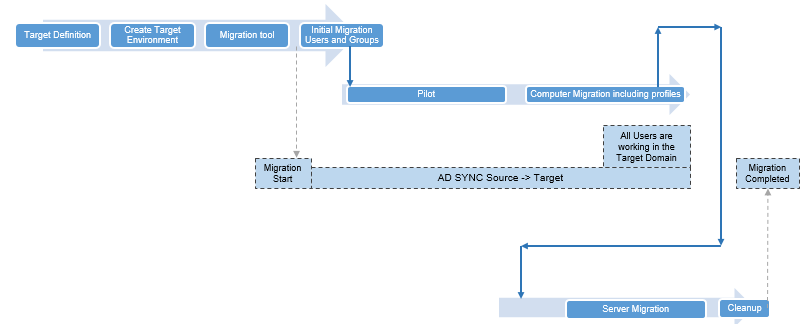


Figure – III

Migration flow of AD migrator:

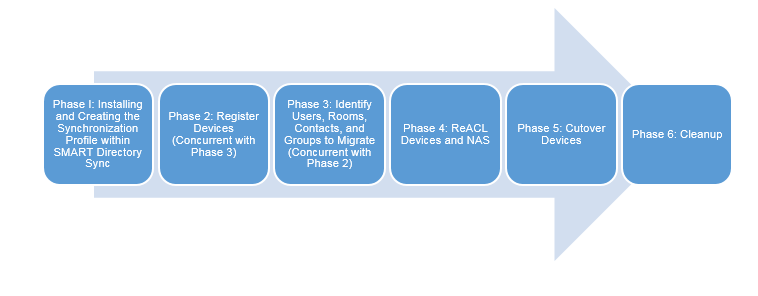
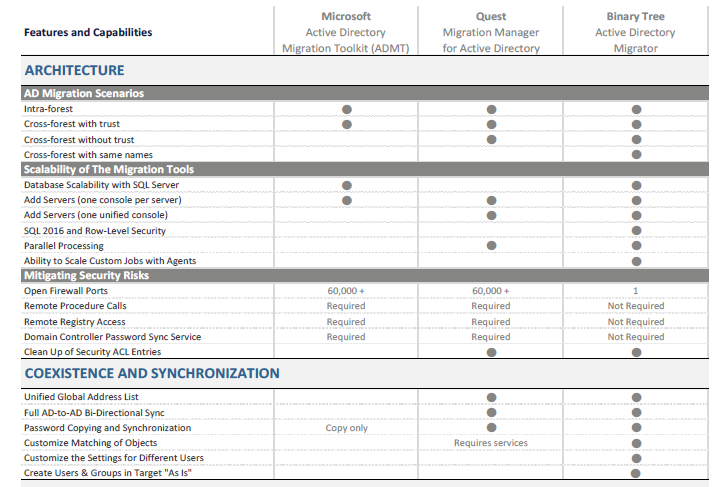
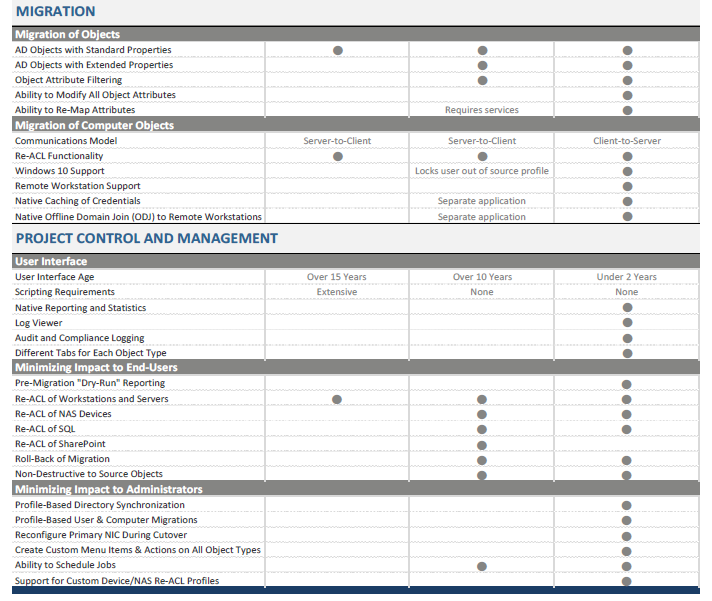


Figure – IV

Comparison table of ADMT, AD Migrator and QMM:

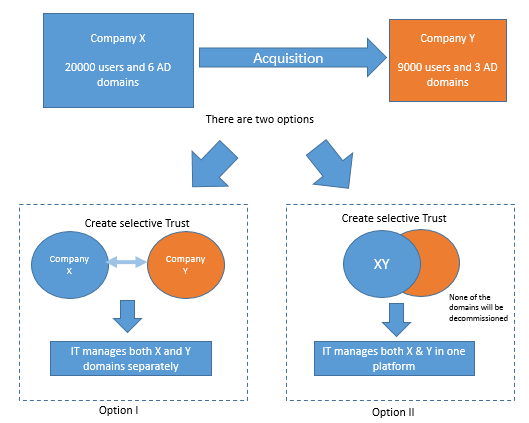




* + 1. Conducting a pilot project with a small number of users and resources, starting slowly and increasing velocity as the pilot achieve success
    2. Creating backup and recovery plans for unexpected issues that arise during the migration, allowing you to restore the previous AD environment without impacting users and organizational workflow
    3. Anticipating risks and establishing plans to address them
    4. Define the end state of active directory infrastructure
       1. Acquisition – Inter-forest consolidation

Option I: IT manages both X and Y in the separate platforms in the post-acquisition.

Option II: Migrate AD resources from company Y to AD in company X in the post-acquisition. Finally decommission AD domain of company Y.



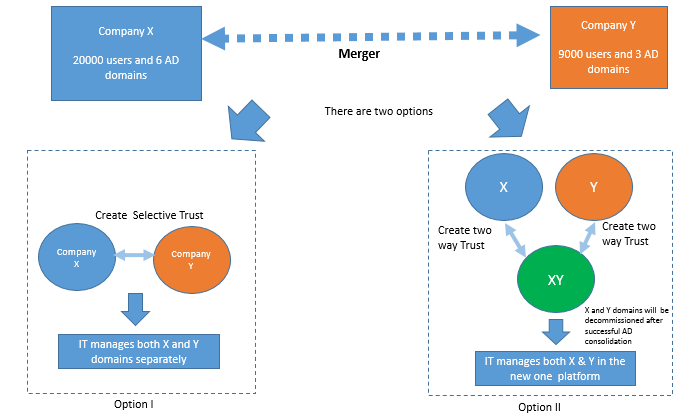
**Figure V**

* + - 1. Merger – Inter-forest consolidation

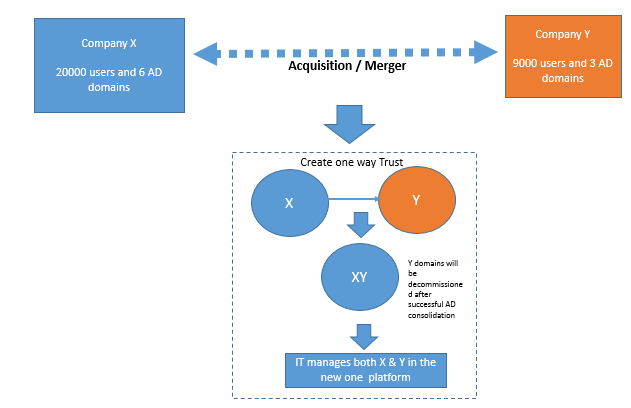
Option I: IT manages both X and Y in the separate platforms in the post -merger.

Option II: Migrate both the AD resources (company X and company Y) into the new AD environment in the post -merger. Finally decommission AD domains of both the companies. IT manages X and Y in the single platform.

Option III: Migrate the AD resources of company Y into the company X in the post -merger. Finally decommission AD domain of company X. IT manages XY in the single platform.

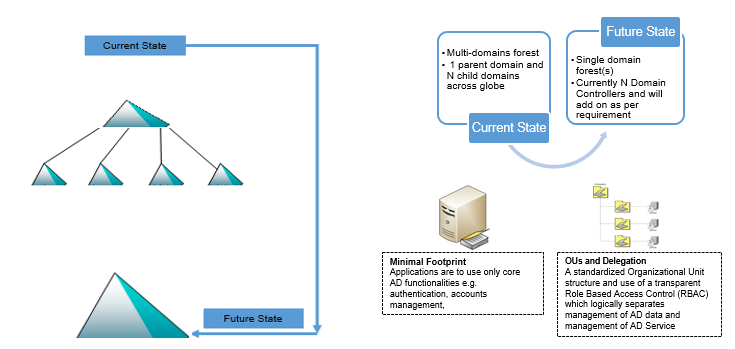


**Figure - VI**

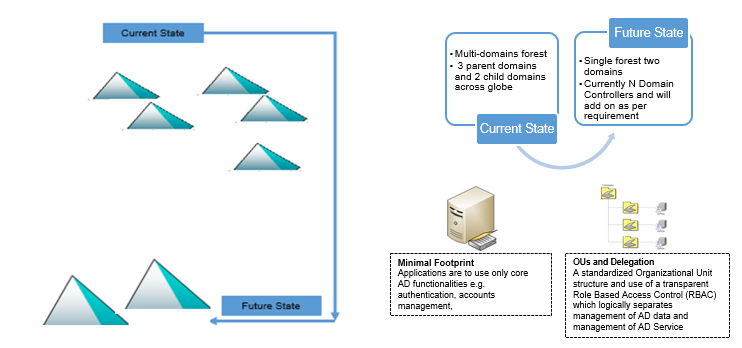


**Figure - VII**

* + - 1. Consolidate child domains/multiple domains into parent domain
* Consolidate AD resources from the child domains into the parent domain in the post-consolidation. Finally decommissions of unwanted child domains.
* Consolidate AD resources from the multiple parent domains and child domains into the parent domains in the post-consolidation. Finally decommissions of unwanted domains.



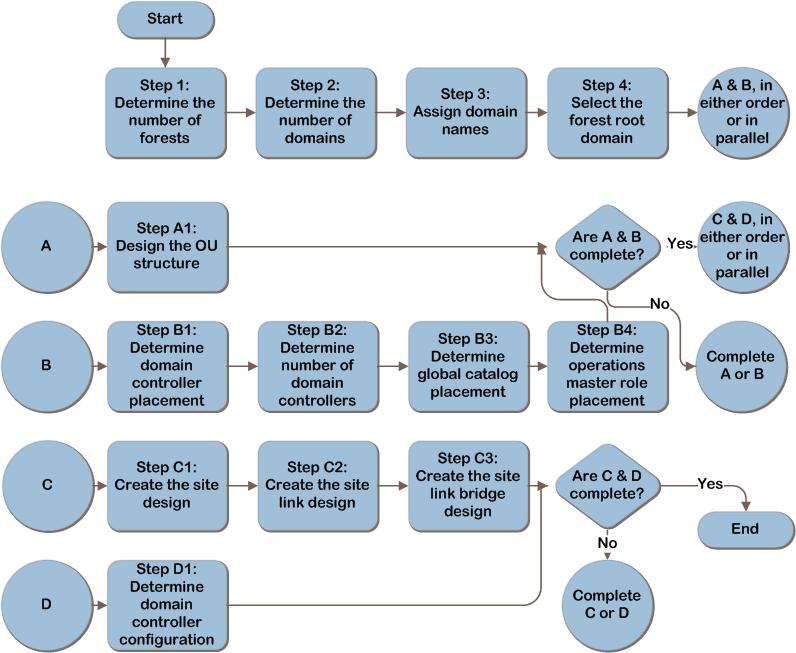
**Figure – VIII**



**Figure – IX**

* + - 1. Flowchart for creating new target domain.

Following diagram represents the steps to create new AD domain.



**Figure – X**

* + 1. Created a checklist for the active directory consolidation using AD migration tool
* Inter-forest consolidation (acquisition or merger)
  + If IT manages both the company X and company Yin the separate platforms as per the company agreement and requirement, then selective trust will be created between X and Y in both the AD domains. None of the AD domain will be decommissioned. Refer Figure V, VI (option I).
  + If AD resources of both the company Y and company X will be managed by IT in the single platform, then two-way trust will be created and none of the AD domains will be decommissioned. Refer Figure VI (option II)
  + If AD resources of company X and company Y will be migrated to the new AD environment and finally AD domains of the company X and company Y will be decommissioned, then IT manages both the company X and company Y in the new single platform. Refer figure VI (option II) & figure –X. Also refer 4.2.11.1.
  + If AD resources of the company Y will be migrated in the AD environment of company X and finally AD domain of the company Y will be decommissioned, then IT manages both the company X and company Y in the one platform. Refer figure – VII. Also refer 4.2.11.1.
* Intra-forest consolidation (consolidation of child domains into parent domain)
  + If multiple child domains will be consolidated in the parent domain and finally child domains will be decommissioned, then refer 4.2.11.2 and figure VIII.
  + If multiple domains will be consolidated into one/two domains and finally unwanted domains will be decommissioned, then refer 4.2.11.2 and figure IX.
    - 1. Inter-forest consolidation (acquisition or merger)

Prepare to restructure Active Directory domains within a forest

* Determine your account migration process.
* Assign object roles and locations.
* Develop a test plan for your migration.
* Create a rollback plan.
* Manage users, groups, and user profiles.
* Create a user communication plan.

Prepare the source and target domains

* Setup conditional forwarder in both AD environments for company X and Y.
* Establish trusts that are required for migration.
* Establish migration accounts for your migration.
* Configure the source and target domains for security identifier (SID) history migration.
* Configure the target domain organizational unit (OU) structure.
* Install and configure AD migration tool (AD Migrator or QMM).
* Specify service accounts for your migration.
* Migrate groups
* Migrate MSA, user accounts and workstation account with SID.
* Establish AD sync in the coexistence period.
* Migrate workstation computers including user profiles etc.
* Perform Re-Acling to add the SIDs of the user and group accounts in the target domain.
* Migrate of member servers and user account.
* Migrate local groups.
* Migrate domain controllers.
* Perform re-acling or translate security on member servers.

**Using QMM**

Following diagram represents the process flow of the migration of AD accounts and resources by quest migration manager.

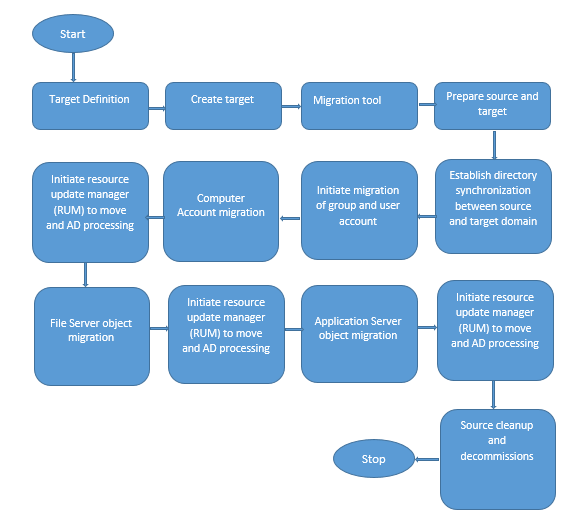


Figure XI

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.

**Using AD Migrator**

<<Will be incorporated>>

* + - 1. Consolidate child domains into parent domain

Prepare to restructure Active Directory domains within a forest

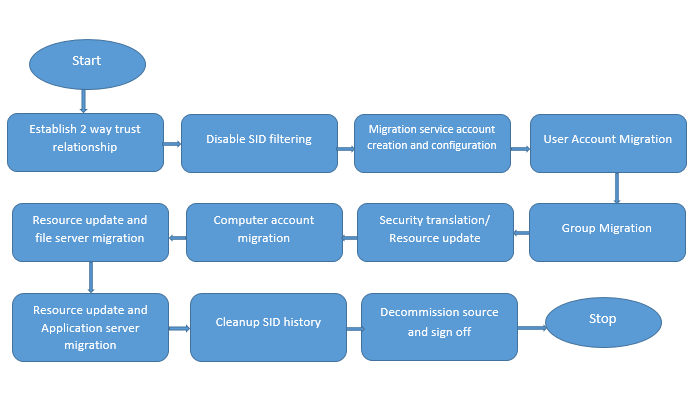
* Determine your account migration process.
* Assign object roles and locations.
* Develop a test plan for your migration.
* Create a rollback plan.
* Manage users, groups, and user profiles.
* Create a user communication plan.

Prepare the source and target domains

* Establish migration accounts for your migration.
* Configure the source and target domains for security identifier (SID) history migration.
* Configure the target domain organizational unit (OU) structure.
* Install and configure AD migration tool (ADMT, AD Migrator or QMM).

**Use ADMT**

Following diagram represents the process flow of the migration of AD account and resources by ADMT tool.



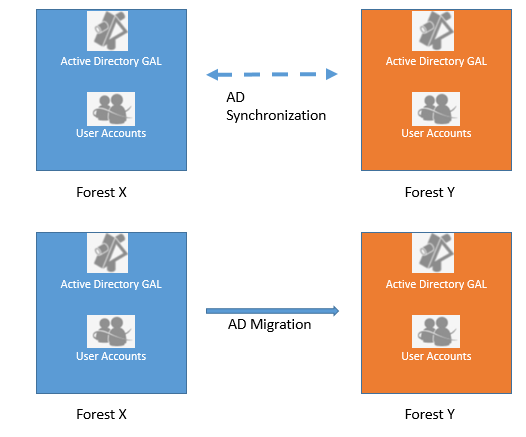
**Figure – XII**

* Specify and transition service accounts using either the Service Account

Migration Wizard or ADMT command-line tools.

* Migrate global groups using either the Group Account Migration Wizard
* Migrate standalone managed service accounts, user accounts, and workstation accounts with their SID histories in batches by User Account Migration.
* Migrate resources, such as member servers and domain local groups. By Computer Account Migration Wizard
* Translate security on servers to add the SIDs of the user and group accounts in the target domain to the access control lists (ACLs) of the resources. by Security Translation Wizard.
* Repeat a migration of user accounts, workstation computers, and member servers, including translating local user profiles to user and computer objects that you migrated earlier.
* Migrate domain local groups using Group Account Migration Wizard
* Migrate domain controllers.
* Translate security on member servers.
  + 1. Maintain active directory synchronization

AD synchronization will be established using AD migration tool during coexistence period of AD, ensuring the productivity of the users.



**Figure – XIII**

* + 1. Maintain on going function and user functionality
    2. Migrate messaging or collaboration platforms
* Active directory migration will impact user access to MS exchange mailboxes and have an impact on an exchange migration.
* Microsoft SharePoint is not as integrated with AD as MS exchange. However, AD migration will frequently impact the SharePoint environment and will require the modification of rights along with modification of user identities.
  + 1. Factors considered during migration of windows servers

Followings critical consideration will be considered during windows server migration in conjunction with AD:

* Security ID's are not portable across member servers.
* Access to files, folders and shares must be maintained during and after both migrations.
* changes must be synchronized during the migrations.
* User access to MAP drives, folders and files must be maintained during and after migration.

Coordinated migration of windows servers and AD environments may be necessary in these situations:

* Replacing domain controllers because of a remote office move
* Converting local users and groups on a server to domain accounts in order to simplify server management
* Consolidating legacy servers to new physical or virtual windows servers for better performance management
  + 1. Sign off
* Hyper Care
* Decommission of domain/forest: Remove last domain controller from the domain/Forest by “On the **Delete the Domain** page, select the option to delete the domain and forest”
* BAU hand over
* Learning and Feedback
  + 1. Appendix