****

2018-2019

**ACTIVE DIRECTORY- <<APP\_NAME>> MIGRATION READINESS**

Contents

[1 Introduction 3](#_Toc525142715)

[2 Objective 3](#_Toc525142716)

[3 Definition & Acronyms 3](#_Toc525142717)

[3.1 Recommended Best Practices 4](#_Toc525142718)

[4 Application components and their Migration strategy 4](#_Toc525142719)

[4.1 Application Name 4](#_Toc525142720)

[4.2 Application Forest Domain Name 4](#_Toc525142721)

[4.3 Application Other Forest Domain Name 5](#_Toc525142722)

[4.4 Application Cross Domain 6](#_Toc525142723)

[4.5 Application Hosted Server Domain 7](#_Toc525142724)

[4.6 Application Host Model, Type 8](#_Toc525142725)

[4.6.1 <<$Web-Based>> 8](#_Toc525142726)

[4.6.3 <<$On-Premise>> 9](#_Toc525142727)

[4.6.5 <<$Cloud>> 10](#_Toc525142728)

[4.6.7 <<$Mainframe>> 11](#_Toc525142729)

[4.6.9 <<$Standalone (Devices)>> 12](#_Toc525142730)

[4.6.11 <<$Other> 13](#_Toc525142731)

[4.7 Client Type 13](#_Toc525142732)

[4.7.1 <<$Thin Client>> 14](#_Toc525142733)

[4.7.3 <<$Thick Client>> 14](#_Toc525142734)

[4.7.5 <<$Thin and Thick Client>> 15](#_Toc525142735)

[4.7.7 <<$Citrix (HVD)>> 16](#_Toc525142736)

[4.7.9 <<$Web Browser/Service>> 17](#_Toc525142737)

[4.8 Application SSL Certificate 18](#_Toc525142738)

[4.9 Application Service Account 19](#_Toc525142739)

[4.10 File and Registry Permissions 21](#_Toc525142740)

[4.10.1 <<$None>> 21](#_Toc525142741)

[4.10.2 <<$Dynamic File Structure>> 21](#_Toc525142742)

[4.10.3 <<$Registry Permission>> 22](#_Toc525142743)

[4.10.4 <<$NAS>> 23](#_Toc525142744)

[4.10.5 <<$SAN>> 23](#_Toc525142745)

[4.11 Application Distribution List Mailbox 24](#_Toc525142746)

[4.11.1 <<$Distribution List>> 24](#_Toc525142747)

[4.11.2 <<$Shared Mailbox>> 25](#_Toc525142748)

[4.11.3 <<$Distribution List and Shared Mailbox>> 26](#_Toc525142749)

[4.12 Application Share Point 27](#_Toc525142750)

[4.13 Authentication Mechanism 27](#_Toc525142751)

[4.14 Application Access Method 32](#_Toc525142752)

[4.14.1 <<$Direct Application Access>> 32](#_Toc525142753)

[4.14.2 <<$Based on Group membership>> 33](#_Toc525142754)

[4.14.3 <<$Based on Rule/Policy>> 34](#_Toc525142755)

[4.14.4 <<$Other>> 35](#_Toc525142756)

[4.15 Application Authentication Type 36](#_Toc525142757)

[4.15.1 <<$Service\_Accounts>> 36](#_Toc525142758)

[4.15.2 <<$Virtual\_Directory\_Service (VDS+)>> 37](#_Toc525142759)

[4.15.3 <<$CA\_SiteMinder>> 38](#_Toc525142760)

[4.15.4 <<$Enterprise\_Sec>> 39](#_Toc525142761)

[4.15.5 <<$Gateway (ESG)>> 40](#_Toc525142762)

[4.15.6 <<$Ping\_SSO>> 41](#_Toc525142763)

[4.15.7 <<$Centrify>> 42](#_Toc525142764)

[4.15.8 <<$ADFS>> 43](#_Toc525142765)

[4.15.9 <<$Essso>> 44](#_Toc525142766)

[4.15.10 << $Other>> 45](#_Toc525142767)

[4.15.11 << $Does not use AD for any authentication>> 46](#_Toc525142768)

[4.16 Local Accounts Creation 46](#_Toc525142769)

[4.16.1 <<$Yes>> 46](#_Toc525142770)

[4.16.2 <<$No>> 47](#_Toc525142771)

[4.17 Application Dependency 47](#_Toc525142772)

[4.17.1 <<$Yes>> 47](#_Toc525142773)

[4.17.2 <<$No>> 48](#_Toc525142774)

[2 Migration Wave/s 48](#_Toc525142775)

[3 References 49](#_Toc525142776)

[3.1 Request for new server 49](#_Toc525142777)

[3.2 Request for new service/technical account 49](#_Toc525142778)

[3.3 Request for local share 49](#_Toc525142779)

[3.4 Request for shared mailbox 49](#_Toc525142780)

[3.5 Request for new DL 49](#_Toc525142781)

[3.6 Request for file/folder/registry permissions 49](#_Toc525142782)

[3.7 Support Information 49](#_Toc525142783)

# Introduction

Active directory migration program aims to simplify the complex Active Directory environment in Fidelity. As part of the program, three domains (DMN1, FMRCO and DSDOM1) are transformed into one domain (WINROOT). The applications and infrastructures residing on these legacy domains will be impacted due to the transformation and they need to be migrated to the WINROOT domain.

# Objective

The objective of this document is to provide a comprehensive guide for the application migration. It includes all the AD dependent components that the application uses, and the steps that you need to follow in order to migrate each component to the new domain.

# Definition & Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AD | Active Directory |
| DN | Domain Name |
| FQDN | Fully qualified domain name |
| DB | Database |
| DFS | Dynamic File Structure |
| GPOs | Group Policy Object |

## Recommended Best Practices

Identify all places (property file, config file etc.) where IP address of AD domain is used and change it with FQDN of AD domain

# Application components and their Migration strategy

## Application Name

Name of this Application is **<<$Application\_Name>>** and the below are the migration considerations for the application.

## Application Forest Domain Name

Application uses Forest Domain **<<$Yes>>**

This application is integrated with **<<$Forest\_Domain\_Name>> Forest**, Please find the below Considerations and Migration Strategy.

#### Assessment Response

Based on Application Assessment for Active Directory Integrations, Active Directory domain name where application is registered are <<xxxxxxxxx >>. Details are collected from your Application Team, Owner at DTM SAM survey. Please validate the correct domain names <<xxxxxxxxx >>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all Places in the Application e.g. source code, configurations, servers where current AD Domain <<xxxxxxxxx >> is used
* Plan for changing your Application configurations, servers, source code connecting new AD Domain after new AD is available

#### Migration strategy

Where legacy AD domain values are used in application configuration they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to;

* Consult AD, Application Remediation team before making changes
* Change Application source code, configurations related to AD domain authentication, AD groups and group membership
* Change Application Server connectivity details for new AD domain trust e.g. One way trust, two way domain trust
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing.

## Application Other Forest Domain Name

Application uses Other Forest Domain **<<$Other>>**

#### Assessment Response

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below.

Please validate Other Domain Details **<< Large Text>>**

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all Places in the Application e.g. source code, configurations, servers where current AD Domain <<xxxxxxxxx >> is used
* Plan for changing your Application configurations, servers, source code connecting new AD Domain after new AD is available

#### Migration strategy

Where legacy AD domain values are used in application configuration they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to;

* Consult AD, Application Remediation team before making changes
* Change Application source code, configurations related to AD domain authentication, AD groups and group membership
* Change Application Server connectivity details for new AD domain trust e.g. One way trust, two way domain trust
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing.

## Application Cross Domain

Application uses Cross Domain **<<$Yes>>**

#### Assessment Response

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below.

Please validate Cross Domain Details **<< Large Text>>**

This application integrated with cross Domains, Please find the below Considerations and Migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all Places in the Application e.g. source code, configurations where *AD cross domain authentication, AD groups and group membership is used*
* Identify all places where *host details (FQDN, DN, host, port etc.)* are used in your Application configuration
* Identity all Places in the Application e.g. Servers where *AD cross domain trust* is used
* Are there authentication dependency on a local login script being executed

#### Migration strategy

Where legacy AD domain values are used in application configuration they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes
* Change Application source code, configurations related to AD cross domain authentication, AD groups and group membership
* Change Application Server connectivity details for new AD cross domain trust e.g. One way trust, cross domain trust
* Perform the necessary testing and BCP testing.

#### <<$No>>

This application does not integrate with cross Domains so no changes are required.

## Application Hosted Server Domain

Application hosted/deployed on Server AD domain <**<$Yes>>**

#### Assessment Response

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below.

Your Application is hosted/deployed servers connected to any of these active directory Domains (DMN1, FMRCO and DSDOM1). Please validate the correct domain names DMN1, FMRCO and DSDOM1 where your Application Server is connected

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all Application Hosted Server Lists, FQDN, IP Address
* Validate Application Server DNSHostName ‘s e.g. <abcd. im.fmrco.com> uses what DistinguishedName’s e.g.
  + < CN=abcd,OU=Domain Controllers,DC=im,DC=fmrco,DC=com>
  + <CN=xyz,OU=Servers,OU=FMRCO,OU=US,DC=im,DC=fmrco,DC=com>
  + <CN=mno, OU=Workstations,OU=FIMT,OU=FMRCO,OU=US,DC=im,DC=fmrco,DC=com>
  + < CN=def,OU=Computers,OU=Unix,DC=im,DC=fmrco,DC=com>
* Plan for changing your Application Hosted Server DNSHostName connecting new AD Domain after new AD is available

#### Migration strategy

Where legacy AD domain values are used in application hosted server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Change Application Server connectivity details for new AD cross domain trust e.g. One way trust, cross domain trust till the time your Application Server migrated to new Servers e.g. your new server DNSHostName will change to “cn=abcd, OU=xyz, DC=RootDomain,DC=com”

#### <<$No>>

Application doesn’t hosted/deployed servers connected to any of these active directory Domains (DMN1,FMRCO and DSDOM1), no changes are required

## Application Host Model, Type

Application host model <**<$Yes>>**

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below

This application is of type <**<$Host\_Model>>** Application**,** please find the below Considerations and migration strategy.

## <<$Web-Based>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* If your web server is on non-windows operating system then continue with the existing operating system
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server e.g. IIS Web Server App Pool to run the webservice under Service account. Review IIS Webserver, ASP .NET projects configuration files to gather Application Pool e.g. find out any Service Account, RoleGroup Mapping configurations like below

<authorization>

<allow role="domain\R-APP-groupname-M" />

<allow user="\*" />

</authorization>

* Identity all service/technical accounts are used to authenticate against Legacy AD

#### Migration strategy

Where legacy AD domain values are used in application Web server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server
* Change all service/technical accounts are used to authenticate against Legacy AD and connect to new AD
* Perform the necessary testing and BCP testing

## <<$On-Premise>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* If your web server is on non-windows operating system then continue with the existing operating system
* Please check on-premise server is connected to any of AD Domain which require migration post new AD domain is available
* Identify all places in your on-premise deployment where Service Accounts, Hardcode AD details (host and port) or hardcoded IP address is used

#### Migration strategy

Where legacy AD domain values are used in application on-premise server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server
* Change all service/technical accounts are used to authenticate against Legacy AD and connect to new AD
* Perform the necessary testing and BCP testing

## <<$Cloud>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please identify if your Cloud Application is accessed by on-premise Federated Authentication such as Active Directory Federation Service (ADFS)
* Please identify if your cloud hosted server, cloud application uses any on-premise Legacy AD domain objects such as Service Accounts, AD Groups and other objects from AD container

#### Migration strategy

Where legacy AD domain values are used in your Cloud application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If on-premise federated authentication is used, plan for changing Authentication, Authorization parameters
* Plan for changing Cloud Application hosted server connecting new AD domain
* Perform the necessary testing and BCP testing

## <<$Mainframe>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check Mainframe Application Authentication process such as does the Application uses local mainframe authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Please check if AD accounts, AD groups are provisioned to Mainframe Application by Identity Management Tool
* Identify places in Mainframe Application where AD objects if used

#### Migration strategy

Where legacy AD domain values are used in your Mainframe application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Mainframe Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain
* Consult Identity Management team if changes are made for User Provisioning of new AD accounts, groups from new AD
* Perform the necessary testing and BCP testing.

## <<$Standalone (Devices)>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check your Application Authentication process such as does the Application uses local device authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application e.g. any webservice, API call

#### Migration strategy

Where legacy AD domain values are used in application Web server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web service, API call
* Perform the necessary testing and BCP testing.

## <<$Other>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check your Application Authentication process such as does the Application uses local device authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application
* Identify all places in your Application deployment where Service Accounts, Hardcode AD details (host and port) or hardcoded IP address is used

#### Migration strategy

Where legacy AD domain values are used in application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server
* Change all service/technical accounts are used to authenticate against Legacy AD and connect to new AD
* Perform the necessary testing and BCP testing

## Client Type

Type of client is presented to end users <**<$Yes>>**

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below

This application presents <**<$ Client\_Type >>** as Client type when users access the Application. Please find the below Considerations and migration strategy.

## <<$Thin Client>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations e.g. any webservice, API call
* Identity all service/technical accounts, AD Groups are used to authenticate against Legacy AD

#### Migration strategy

Where legacy AD domain values are used in application Thin Client they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in your Application Thin Client connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain e.g. change Service Account, AD Groups, AD container
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application thin client e.g. web service, API call
* Perform the necessary testing and BCP testing.

## <<$Thick Client>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations e.g. any webservice, API call
* Identity all service/technical accounts, AD Groups are used to authenticate against Legacy AD

#### Migration strategy

Where legacy AD domain values are used in application Thick Client they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in your Application Thick Client connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain e.g. change Service Account, AD Groups, AD container
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application thin client e.g. web service, API call
* Perform the necessary testing and BCP testing.

## <<$Thin and Thick Client>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations e.g. any webservice, API call
* Identity all service/technical accounts, AD Groups are used to authenticate against Legacy AD

#### Migration strategy

Where legacy AD domain values are used in application Thin, Thick Client they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in your Application Thin, Thick Client connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain e.g. change Service Account, AD Groups, AD container
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application thin client e.g. web service, API call
* Perform the necessary testing and BCP testing.

## <<$Citrix (HVD)>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please identity current Citrix Authentication process against Legacy AD Domain e.g. does Citrix uses federated authentication using ADFS (Active Directory Federation Service)
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Citrix Application Configurations
* Please validate if Citrix Application Hosted Server is AD Domain Joined
* Please validate if Citrix Application provide desktop single sign on using Kerberos
* Identity all service/technical accounts, AD Groups are used to authenticate against Legacy AD

#### Migration strategy

Where legacy AD domain values are used in Citrix application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in your Citrix Application connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Migrate Citrix Application Hosted Server to connect new AD Domain
* Change all service/technical accounts are used to authenticate against Legacy AD and connect to new AD
* Change configurations related to desktop single sign on using Kerberos
* Change other AD detail (FQDN, host and port) or hardcoded IP address to connect new AD Domain
* Perform the necessary testing and BCP testing

## <<$Web Browser/Service>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. Currently assessment for 135 domain controller and 3 AD Domain is in progress.

After assessment new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all service/technical accounts, AD Groups are used to authenticate against Legacy AD
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used
* Identify if Application requires Integrated Windows Authentication (IWA) to be enabled in Browser connecting to Legacy AD Domain

#### Migration strategy

Where legacy AD domain values are used in application Service they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in your Application connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* Change Integrated Windows Authentication (IWA) configurations connecting to new AD domain
* Change other AD detail (FQDN, host and port) or hardcoded IP address to connect new AD Domain for the services which used Legacy AD domain
* Perform the necessary testing and BCP testing

## Application SSL Certificate

Application uses SSL Certificates **<<$Yes>>**

#### Assessment Response

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below.

Please validate all Certificates, which are registered against active directory domain

All Certificates Details **<< Large Text>>**

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Validate all SSL Certificates Issue Date, Expiry Date, Root CA, Intermediate CA details
* Validate if SSL Certificate is issued from Internal Active Directory Certificate Service (ADCS) and from to which Legacy AD domain
* Validate if SSL certificate is used from external 3rd Party ADCS such as Verizon and does the external certificate has any internal ADCS dependency
* Identity if SSL certificates are stored at Key Store such as Java Key Store (JKS) and protected by secret encryption keys. Also validate if SSL certificates are managed centrally at HSM (Hardware Security Module)
* Validate if SSL Certificates are used for One way SSL Or Two Way SSL Authentication by Applications before allowing Users access to Applications
* Identity all Client side and Server side SSL certificates
* Identity if WebServices, API’s use SSL certificates for signing, authenticating services

#### Migration strategy

Where legacy AD domain values might be used by SSL certificates they will need to be replaced with new SSL certificates from new AD domain. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes
* Request new SSL Certificate from new Internal Active Directory Certificate Service (ADCS) and from new AD domain
* Import new SSL Certificate to Key Store such as Java Key Store (JKS), HSM
* Make changes to Application for One way SSL Or Two Way SSL Authentication
* Change all Client side, server side certificates and new SSL certificates
* Change WebServices, API’s for new SSL certificates and for signing, authenticating services
* Perform the necessary testing and BCP testing.

#### <<$No>>

This application does not use SSL certificate so no changes are required.

## Application Service Account

Application uses Service Accounts **<<$Yes>>**

#### Assessment Response

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below.

Please validate all service accounts / operational accounts created in Legacy active directory domain to administrate your application

All Service Accounts Details **<< Large Text>>**

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity all Service Accounts used by Data bases such as Service Accounts used to Authenticate/Start/Stop Databases e.g. Service Account Name “SA-SQL-P” and associated SQL Global Permission Group (R-) e.g. Prefix-SQLServer-Database-AccessLevel "R-SQL-AllSQLServers-X"
* Identity all Service Accounts used to run Service to Service Level Authentication e.g. SPN set for Kerberos Authentication which enables Kerberos to securely communicate with the Service such as setspn –s ABCDAppService/ServerAddress domain\ SA-ServiceAccount. And associated Service Permission Group e.g. Prefix-SERVER-ServiceDisplayName-AccessLevel “P-SMPWEBM05-ComputerBrowser-R”
* Identity all Service Accounts for running HTTPS(web) on Server which requires Service Account seamless access e.g. setspn –s HTTPS/ServerAddress domain\ SA-ServiceAccount
* Identity all Domain Security Groups e.g. SCSM and associated Service Accounts used at Application Hosted Server
* Identity all Application pool with the service account to run the web service under that SA account e.g. Role Group, Service Account configurations in IIS configuration files
* Identity all Service Accounts used by Identity Access Management Tools which requires Service Accounts to run, authenticate service against Legacy AD domain such as ADFS, Microsoft Identity Manager, ADAM, Active Role Server and all others

#### Migration strategy

Where Service Accounts from legacy AD domain might be used they will need to be replaced with new Service Accounts from new AD domain. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes
* Changes Service Accounts configurations from new AD Domain to run Data bases
* Change Service Accounts configurations from new AD Domain to run services to service communication
* Change Service Accounts configurations from new AD Domain for running HTTPS(web) on Server
* Change Service Accounts configurations from new AD Domain part of Domain Security Groups
* Change Service Accounts configurations from new AD Domain to run Application Pool
* Change all Service Accounts configurations from new AD Domain for LDAP services, IAM services
* Perform the necessary testing and BCP testing.

#### <<$No>>

This application does not use Service Accounts so no changes are required.

## File and Registry Permissions

## <<$None>>

Application doesn’t use any File and Registry Permission, no change is required.

## <<$Dynamic File Structure>>

This Application uses Dynamic files Structure, Please find the below Considerations and migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify full name and path of the file which application uses e.g. names of DFS Paths, UNC Paths
* Identify the Service accounts used to access the DFS
* Identify system or domain hosting file on file server which uses Legacy AD Domain
* Identity all File Permission Group e.g. Prefix-Server-FolderandFilePath[(#)]-AccessLevel "P-SMPFILEP01-D-Data-Employee Benefits-HR-Documentat-W2.Doc(1)-RW"
* Identity all Folder Permission Group e.g. Prefix-Server-Folder Path[(#)]-Access Level "P-SMPWEBM05-D-Apps-Siebel-Rx"
* Identity all Server Share Permission Group e.g. Prefix-Server-ShareName-AccessLevel "P-SMPWEBM05-APPS-R"
* Identity all DFS Folder Permission Group e.g. Prefix-Domain-DFS Root-DFS Link Name/Folder Path -AccessLevel "P-C-AllLocations-AllDepartments-R"

#### Migration strategy

Where Dynamic files Structure, groups, service accounts from legacy AD domain might be used they will need to be replaced with DFS, Service Accounts, and Groups from new AD domain. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes
* Make changes to system or domain hosting file on file server connecting new AD Domain
* Make changes to All Service Accounts, File Permission Group, Folder Permission Group, Server Share Permission Group, DFS Folder Permission Group connecting new AD Domain
* Make changes to full name and DFS Paths, UNC Paths of the file
* Arrange for necessary testing and BCP testing.

## <<$Registry Permission>>

This Application uses Registry Permission, Please find the below Considerations and migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all file/folder/registry permissions and GPOs required for the application
* Identify all Registry Permission Group in Legacy AD Domain e.g. Prefix-Server-FullNameRegistryEntry[(#)]-AccessLevel "P-SMPWEBM05-HKLMSYSTEMCurrentControlSetServiceslanmans(1)-R"
* Identity Registry entry in your Application Server, any hardcoded Legacy AD detail (FQDN, host and port) or hardcoded IP address is used

#### Migration strategy

Where Registry Permission Group, AD entries from legacy AD domain might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes
* Make changes to registry permissions connecting new AD Domain in your Application hosted Server
* Make changes to Registry Permission Group
* Make changes to hardcoded Legacy AD detail (FQDN, host and port) or hardcoded IP address in Registry connecting new AD Domain
* Arrange for necessary testing and BCP testing.

## <<$NAS>>

This Application uses NAS, Please find the below Considerations and migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify names along with FQDN (Fully qualified domain name) of Network storage server or NAS used by application.
* Identify how Network storage is associated with application

#### Migration strategy

Where Network storage server or NAS from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Application uses Network Storage to store data manually or triggered by an event after authenticating against AD. Make sure each of the storage components and servers where this storage is installed are migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Note** – To request registration of new storage servers on a new AD domain, raise a request.

## <<$SAN>>

This Application uses SAN, Please find the below Considerations and migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify names along with FQDN (Fully qualified domain name) of Network storage server or SAN used by application.

#### Migration strategy

Where SAN from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Application uses Network Storage to store data manually or triggered by an event after authenticating against AD. Make sure each of the storage components and servers where this storage is installed are migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Note** – To request registration of new storage servers on a new AD domain, raise a request.

## Application Distribution List Mailbox

This application uses Distribution List Mailbox **<<$Yes>>**for communication, Please find the below Considerations and migration strategy.

## <<$Distribution List>>

This Application uses Distribution List, Please find the below Considerations and migration Strategy

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please Identity names of DL's your Application uses, DL's requested and members of your DL's
* Identify distribution groups used by Application from Legacy AD
* Identify names along with full SMTP address of DL or mail group used by application

#### Migration strategy

Where DL’s from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Make changes to DL Groups used at Application and connect to new AD
* Make changes to SMTP address of DL or mail group used by application
* Perform necessary testing and BCP testing.

**Note** – To request creation of new DL or mail group on a new AD domain, refer section **'Request for new DL**'

## <<$Shared Mailbox>>

This Application uses Shared Mailbox, Please find the below Considerations and migration Strategy

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify DS- groups will be used for sending e-mail communication (mail enabled) and for granting access to shared mailboxes (MB-)
* Identify names along with full SMTP address of shared mailbox used by application.
* Identify how the access to these shared mailboxes is requested by a user. (ex. SNOW or on mail etc.)

#### Migration strategy

Where Shared Mailbox from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Make changes shared mailboxes which are to be migrated to the new AD domain
* Make changes to Application Configurations related to new Shared Maiboxes
* Perform the necessary testing and BCP testing.

**Note** – To request creation of shared mailbox on new AD domain, Refer section '**Request for shared mailbox'**

## <<$Distribution List and Shared Mailbox>>

This Application uses both Distribution List and Shared Mailbox, Please find the below Considerations and migration Strategy

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Identify names along with full SMTP address of DL or mail group used by application.
* Identify names along with full SMTP address of shared mailbox used by application.
* Identify how the access to these shared mailboxes is requested by a user. (ex. SNOW or on mail etc)

#### Migration strategy

Where DL’s from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Make changes to DL Groups used at Application and connect to new AD
* Make changes to SMTP address of DL or mail group used by application
* Make changes shared mailboxes which are to be migrated to the new AD domain
* Make changes to Application Configurations related to new Shared Maiboxes
* Perform the necessary testing and BCP testing.

**Note** – To request creation of new DL or mail group on a new AD domain, refer section **'Request for new DL**' and To request creation of shared mailbox on new AD domain, Refer section '**Request for shared mailbox'**

#### <<$None>>

Application doesn’t using any DL or Share mailbox, no changes are required.

## Application Share Point

This application uses Shared Point **<<$Yes>>**for Documents Library, content management Please find the below Considerations and migration strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify how SharePoint access is provided to users of your Application and Do all users of your Application get access to SharePoint
* What are the different types of users and how is the access classification done for them
* Identity all SharePoint AD Groups from Legacy AD Domain

#### Migration strategy

Where SharePoint connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD team for SharePoint migration Plan to the new AD domain
* Make Changes to your Application configurations for new SharePoint URL, Access
* Make Changes to Application specific SharePoint New AD Groups and members of the SharePoint AD Group
* Perform necessary testing and BCP testing.

#### <<$No>>

Application doesn’t using any SharePoint, no changes are required.

## Authentication Mechanism

This application uses Authetication\_Mechanism **<<$Yes>>** as Authentication protocol Mechanism, Please find the below Considerations and Migration Strategy for selected Authentication mechanism.

#### <<$Kerberos>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.
* Identify and Lists all SPN, if SPNs and associated service/technical accounts are used for Kerberos authentication
* Identify all SPN used for Service to Service Authentication across different Application Servers
* Identity all SPN used for HTTPS(web) on Server where Service is running

#### Migration strategy

Where Kerberos Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Make changes to SPN setting connecting new AD Domain and with new lists of Service Accounts
* Change SPNs for Kerberos Authentication for Service to Service Communication
* Change SPNs used for HTTPS(web) on Server where Service is running
* Register the new host in new AD domain and setup Kerberos authentication.
* Perform the necessary testing and BCP testing.

Please refer section " **Request for new service/technical account** " for details.

#### <<$NTLM>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Service/technical accounts are used for authentication
* Identity your Application Server configurations for NTLM related settings
* Identity Applications which uses desktop single sign on using NTLM authentication
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server
* If authentication components are installed on a non-windows operating system then continue with the existing operating system

#### Migration strategy

Where NTLM Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Register the new host in new AD domain and setup Desktop SSO-NTLM authentication.
* Perform the necessary testing and BCP testing.

#### <<$Oauth>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity Federation Server which issues OAUTH token for Identity Server and whether Federation server connects Legacy Domain e.g. ADFS 3.0, ADFS 4.0
* Validate if OAUTH token contains attributes from Legacy AD Domain
* Identity all possible Legacy AD domain objects such as AD container, AD Groups, Service Accounts

#### Migration strategy

Where OAUTH Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult Identity Management Federation Service for OAUTH related configurations that are needed in your Application
* Register the new host in new AD domain and setup OAUTH authentication
* Perform the necessary testing and BCP testing.

#### <<$OpenID>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity Federation Server which issues OpenID token for Identity Server and whether Federation server connects Legacy Domain e.g. ADFS 3.0, ADFS 4.0
* Validate if OpenID token contains attributes from Legacy AD Domain
* Identity all possible Legacy AD domain objects such as AD container, AD Groups, Service Accounts

#### Migration strategy

Where OpenID Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult Identity Management Federation Service for OpenID related configurations that are needed in your Application
* Register the new host in new AD domain and setup OpenID authentication
* Perform the necessary testing and BCP testing.

#### <<$SAML>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity Federation Server which issues SAML token for Identity Server and whether Federation server connects Legacy AD Domain e.g. ADFS 3.0, ADFS 4.0
* Validate if SAML token contains attributes from Legacy AD Domain
* Identity all possible Legacy AD domain objects such as AD container, AD Groups, Service Accounts

#### Migration strategy

Where SAML Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult Identity Management Federation Service for SAML related configurations that are needed in your Application
* Register the new host in new AD domain and setup SAML authentication
* Perform the necessary testing and BCP testing.

#### <<$Other>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify what are other Authentication Protocol used such as HTTPS (SSL Certificate), BASIC Authentication, FORM based Authentication used where Legacy AD Domain is used for Authentication
* Identify application used AD authentication through headers, custom tokens
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server
* Identity all Service Accounts, AD Domain Security Groups in your Application from Legacy AD Domain

#### Migration strategy

Where Other Authentication connecting legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Make changes for HTTPS, BASIC AUTH, FORM Based Authentication
* Make Changes related to Service Accounts, Domain Security Groups connecting new AD Domain
* Perform the necessary testing and BCP testing.

#### <<$None>>

* Application doesn’t use authentication mechanism which are Legacy AD dependent , no change required

## Application Access Method

## <<$Direct Application Access>>

This application is accessible by users where Legacy AD user ID created directly in the Application Database

Please find the below Considerations and Migration Strategy

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if application is accessed directly by users using Legacy AD User Id. List if there are any exceptions.
* Identify how the access to this application is requested by a user.
* Identify any Identity Management Tool Provisions Legacy AD User ID to this Application Database

#### Migration strategy

Where User ID from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD team post AD Migration will there be change in AD User ID, DN of User ID
* Consult Identity Management team if there will change in User Provisioning/De-Provisioning Process to delete/update new AD User ID in Application Database
* Make changes to your Application source code, configurations connecting new AD domain for Authentication, Authorization
* Perform necessary testing and BCP testing.

## <<$Based on Group membership>>

This application is accessible based on Legacy AD domain group membership, Please find the below Considerations and Migration Strategy

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Role Groups (R-) e.g. domain global groups, which are used to group user accounts which simplify granting access to Users
* Identify Permission Groups (P-) e.g. all Application Permission Group, all SQL Global Permission Group, all Service Permission Group, all Folder Permission Group, all File Permission Group, all Server Share Permission Group used from Legacy AD Domain
* Identity if Application Portal Server has configured Legacy AD domain for Group Based authorization for Portlets, Pages, Entitlements
* Identity if your Application Manages AD Groups in Application Database, how the AD groups are synchronized from Legacy AD domain

#### Migration strategy

Where User ID from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Permission Groups, Role Groups
* Make changes to your Application Portal Server Configurations related to new AD configuration for Group based authorization of Pages, Portlets, Entitlements
* Perform necessary testing and BCP testing.

## <<$Based on Rule/Policy>>

This application is accessible based on Rule/Policy, Please find the below Considerations and Migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity if your Application Dependent on GPO (Group Policy Object), defined group of users, computer accounts from any existing Legacy AD Domain, Domain Controller
* Identify if your Application Server dependent on Legacy AD Forests network based on defined rules such as Server Access based One-Way trust established with AD Forest
* Identity the Rules/Policy which are used in segregation of functionality and access to application by any means (e.g. registry based policy, folder redirection etc.)

#### Migration strategy

Where GPO, Rules, Policy from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for GPO’s, Computer Accounts, Users/Groups
* Make changes to your Application server configurations, re-hosting to connect new AD Domain, use new GPO’s, Computer Accounts
* Request for Rule/Policy configuration on new AD domain for the application
* Perform necessary testing and BCP testing.

## <<$Other>>

This application is accessible based on other method, Please find the below Considerations and Migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all other access method used to connect Legacy AD Domain
* Identify all Service/technical accounts, Local Accounts, Computer Accounts are used for authentication with Legacy AD Domain
* Identity your Application Server configurations for Legacy AD related settings
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server

#### Migration strategy

Where Other Access Method used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Register the new host in new AD domain and test connectivity for authentication.
* Change all places where hardcoded AD detail (host and port) or hardcoded IP address is used
* Change all Service/technical accounts, Local Accounts, Computer Accounts
* Perform the necessary testing and BCP testing.

## Application Authentication Type

This application uses **<<$Authetication\_Type>>** as Authentication Type, Please find the below Considerations and Migration strategy.

## <<$Service\_Accounts>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Service Accounts and Domain Security Groups (Permission Groups ) which are used for
  + Service to Service seamless authentication
  + SQL Server Service Accounts for Service start/stop and access permissions
  + Kerberos Sign on using SPN (service principal name) and Service Accounts
  + IIS Web Server Application Pool configurations using Groups, Service Accounts
  + Service Accounts for running HTTPS(web) on Server which requires Service Account seamless access
  + Service accounts which are member of Folder Permission Group, File Permission Group, Server Share Permission Group, DFS Folder Permission Group, Registry Permission Group
  + Service Accounts used for Firewall Connectivity to Legacy AD Domain
  + Service Accounts used for SFTP Gateway Connectivity to Legacy AD Domain
* Identify all places where hardcoded AD detail (Service Accounts, host and port) or hardcoded IP address is used in your Application server

#### Migration strategy

Where Other Access Method used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Service Accounts, Permission Groups, Role Groups
* Once New Service Accounts and DN of the Service Accounts are available from new AD Domain, unit test the connectivity along with credentials
* Make changes to all the places in your Application Server Machine where Service Accounts need to re-configure, test
* Make changes to all the places in your Application source code, configuration files where Service Accounts need to replaced connecting new AD Domain
* Make changes Domain Security Groups, Permission Groups, and other Admin Groups where Service Account is a member
* Perform the necessary testing and BCP testing.

## <<$Virtual\_Directory\_Service (VDS+)>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify Virtual Directory Server installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Identify if VDS is connected with Legacy AD Domains and AD Objects such as User, Groups, Admin Accounts are synchronized with VDS and Legacy AD Domains
* Identify if VDS is used as Meta Directory between multiple AD Domains and with other target platforms
* Identify if VDS only reads or read/write with Legacy AD domains
* Identify if One or More Applications Reads and Writes to VDS which in turn reads, writes to Legacy AD
* Identify if Authentication, Authorization with VDS are controlled by Legacy AD Domain Objects

#### Migration strategy

Where Virtual\_Directory\_Service (VDS+) used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for VDS such as Re-Hosting VDS to new Windows Server connecting new AD Forest, Domain
* Make changes to connectivity to new AD Domain for AD Objects (Users, Groups, Admin Accounts) Synchronization
* If VDS acts as a Meta Directory with multiple legacy AD Domains, make plan for Users, Groups Synchronization to new AD Domain
* Make changes to VDS for Authentication, Authorization connecting new AD Domain
* Perform the necessary testing and BCP testing.

## <<$CA\_SiteMinder>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Review SiteMinder Integration architecture for legacy AD integrations for Authentication, Single Sign on, Policy/Group based Authorization
* Review SiteMinder Configurations for Legacy AD Domains Integrations
* Identify if SiteMinder is installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Review SiteMinder other Components such as Proxy Server, Federation Server, Policy Server uses any Legacy AD Integrations
* Review SiteMinder Configurations such as Policy Domain, Realm, Request, Response headers if these configurations use Legacy AD Objects such as Users, Groups
* Identify if One or More Applications integrates with CA SiteMinder for Authentication, Course Grained Authorization and Single Sign on with other Web Based Applications
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your CA SiteMinder server

#### Migration strategy

Where CA SiteMinder used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for CA SiteMinder such as Re-Hosting SiteMinder to new Windows Server connecting new AD Forest, Domain
* Consult AD team if CA SiteMinder infrastructure need major changes connecting to new AD Domain or can work with Legacy AD Domain till some time when Legacy AD Domain will sunset/retire/decommission completely
* Plan to make necessary changes for SiteMinder AD connectivity and SiteMinder Configurations
* Plan to coordinate with multiple Applications team for testing, validating Authentication, Authorization Use cases post SiteMinder connectivity is migrated to new AD Doman
* Perform the necessary testing and BCP testing.

## <<$Enterprise\_Sec>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity if Enterprise Security Tool is installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Identify all places where hardcoded Legacy AD detail (host and port) or hardcoded IP address is used in your Enterprise Security server
* Identity all Service Accounts, Admin Accounts used from Legacy AD Domain
* Identify Authentication Methods used to connect Legacy AD Domain
* Identify if Enterprise Security Tool uses desktop security seamless sign on solution using Kerberos, NTLM

#### Migration strategy

Where Enterprise Security Tools used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Enterprise Security Tools such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for new AD Domain Connectivity
* Plan to make changes for hardcoded new AD detail (host and port) or hardcoded IP address is used in your Enterprise Security server
* Plan to make changes all Service Accounts, AD Groups, AD User Tree
* Perform the necessary testing and BCP testing.

## <<$Gateway (ESG)>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity if ESG Gateway Server is installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Identify all places where hardcoded Legacy AD detail (host and port) or hardcoded IP address is used in your ESG Gateway server
* Identity all Service Accounts, Admin Accounts used from Legacy AD Domain
* Identify Authentication Methods used to connect Legacy AD Domain
* Identify if ESG Gateway Server uses desktop security seamless sign on solution using Kerberos, NTLM

#### Migration strategy

Where ESG Gateway used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for ESG Gateway Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for new AD Domain Connectivity
* Plan to make changes for hardcoded new AD detail (host and port) or hardcoded IP address is used in your ESG Gateway server
* Plan to make changes all Service Accounts, AD Groups, AD User Tree
* Perform the necessary testing and BCP testing.

## <<$Ping\_SSO>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity if Ping Federation SSO Server is installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Identify all places where hardcoded Legacy AD detail (host and port) or hardcoded IP address is used in your Ping Federation SSO server
* Identity Ping Federation SSO Server issues SAML, WS-Fed, OAUTH, OpenID token for Ping Federate SSO Server and whether Federation server connects Legacy AD Domain
* Validate if SAML, WS-Fed, OAUTH, OpenID token contains attributes from Legacy AD Domain
* Identity all possible Legacy AD domain objects such as AD container, AD Groups, Service Accounts used by Ping Federation SSO Server
* Identify if One or More Applications integrates with Ping Federation SSO Server for Authentication, Federation Single Sign on with other internal, external partner Applications

#### Migration strategy

Where Ping Federate SSO used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Ping Federate SSO Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Consult AD team if changes to Ping Federate SSO Server re-hosting needed till the time Legacy AD Domain completely retired/decommissioned or can work in parallel
* Plan to make changes for SAML, WS-Fed, OAUTH, OpenID configurations if Ping Federate SSO Server leverages attributes (User, Groups)
* Perform the necessary testing and BCP testing.

## <<$Centrify>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identity if Centrify Server is installed on windows operating system and Windows Server belongs to any existing AD Forests, AD Domains
* Identify all places where hardcoded Legacy AD detail (host and port) or hardcoded IP address is used in your Centrify server
* Identify all Service Accounts, Permission Groups, Security Groups from Legacy AD domain used to run Centrify Services
* Review Centrify Architecture related to legacy AD Integrations such does Centrify require
  + Legacy AD User/Password to Login to Centrify
  + Does Centrify protects privileged accounts from legacy AD such as Service Accounts, Server Admin Accounts, Local Windows Server Accounts
  + Does Centrify provides one time access to Servers Accounts based on Password Rotation Policy
  + Identify how many Windows Server, Admin Accounts managed by Centrify

#### Migration strategy

Where Centrify used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Centrify Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Consult AD team if changes to Centrify Server re-hosting needed till the time Legacy AD Domain completely retired/decommissioned or can work in parallel
* Consult AD team to obtain new List of Service Accounts, Permission Groups from new AD Domain and plan to change the configurations
* Plan to make entire Privileged Account Management process change related to managing Service Accounts, Admin Accounts from all in scope Windows Server
* Perform the necessary testing and BCP testing.

## <<$ADFS>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Review Windows Servers versions and ADFS versions such ADFS 2.0, ADFS 3.0, ADFS 4.0
* Identify all Domain Security/Permission Groups and Service Accounts needed to run ADFS Services
* Identify does ADFS provides all or any Federation protocol such SAML, WS-Fed, OAuth, OpenID
* Identify if Application Authentication, Single Sign on is implemented using Windows Identity Foundation (WIF) which consumes, validates federation protocol from ADFS Server. Also validate Windows Identity Federation Utility is used by Application’s source code, configurations
* Identify Legacy AD Domain OU container for Users, Groups against which ADFS validates Users Credentials
* Validate if ADFS server connected to Legacy all AD Domains or specific AD Domain. Also check if AD one Way Cross Domain Trust or Two way Cross Domain Trust is established

#### Migration strategy

Where ADFS (Active Directory Federation Service) used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for ADFS Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for Domain Security/Permission Groups and Service Accounts needed to run ADFS Services
* Work with Application team for changes, validation and testing need related to Windows Identity Foundation (WIF), Windows Identity Federation Utility
* Plan to make changes for Federation configurations such as attribute, authentication, assertion statement for SAML, WS-Fed, OAuth, OpenID
* Plan to make changes for New AD Domain OU container for Users, Groups against which ADFS validates Users Credentials
* Perform the necessary testing and BCP testing.

## <<$Essso>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Domain Security/Permission Groups and Service Accounts needed to run ESSO (Enterprise Single Sign on) Services
* Identify how many Platforms, Applications uses Enterprise Single Sign on Services
* Identify which are the Legacy AD Domains ESSO server is connected
* Identify Legacy AD Domain OU Containers for Users, Groups against which Users login to Platforms, Applications using ESSO Server Agents
* Identify if for enterprise, desktop SSO solution any Kerberos, NTLM authentication used and any SPN (Service Principal Name) is configured

#### Migration strategy

Where ESSO (Enterprise Single Sign on) Solution used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for ESSO Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for New AD Domain OU Containers for Users, Groups against which Users login to Platforms, Applications using ESSO Server Agents
* Plan to make changes in ESSO server for Service Accounts, Domain Security Groups
* Plan to change all SPN settings for Kerberos constrained delegated authentication
* Perform the necessary testing and BCP testing.

## << $Other>>

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify which Other Authentication Type used such as any centralized Authentication Framework, centralized Single Sign on Framework, Any Custom development Authentication Framework which is integrated with Legacy AD Domain
* Identify if Other Authentication Server/Framework requires any Service Accounts, Admin Accounts, Domain Security Groups from Legacy AD Domain
* Identify Other Authentication Server/Framework use cases related to Legacy AD Domain such as AD OU Container, User Tree, Group Tree
* Identify if Custom Authentication Framework supports Kerberos, NTLM Authentication for which SPNs are set up

#### Migration strategy

Where Other Authentication Server used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Other Auth Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for New AD Domain OU Containers for Users, Groups against which Users login to Platforms, Applications using Other Auth Server
* Plan to make changes in Other Auth server for Service Accounts, Domain Security Groups
* Plan to change all SPN settings for Kerberos constrained delegated authentication
* Perform the necessary testing and BCP testing.

## << $Does not use AD for any authentication>>

Application doesn’t use AD based authentication, no change required

## Local Accounts Creation

## <<$Yes>>

This application use local Computer account, Please find the below Considerations and migration Strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if your Application Deployed on Server which don’t require Admin, Service Accounts from legacy AD Domain
* Identify Application Server hosted machine authentication by Local Computer Accounts and Location Admin Groups
* Validate with legacy Domain AD team if Local Computer Accounts are Synched offline to Legacy AD Domain OU Containers
* Validate Domain Servers of Local Accounts and will have any impact post new AD

#### Migration strategy

Where Local Computer Accounts used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Application Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to make changes for all Local Computer Accounts if these Accounts are synchronized to AD Domain
* Perform the necessary testing and BCP testing.

## <<$No>>

Application doesn’t use any local computer account, no changes are required

## Application Dependency

## <<$Yes>>

This application is having dependency with other application, Please find the below Considerations and migration strategy.

#### Considerations

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to Single Forest and One Root AD domain. As part of Phase 1, assessment for 135 domain controller and 3 AD Domain is in progress.

After Phase 1, new AD domain design will be ready and as part of Phase 2 all Legacy AD domain will be migrated to new AD Domain. Please see below considerations for Application remediation

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Find out which Centralized Authentication Server, Framework has your Application dependent and indirectly uses Legacy AD Domain
* Find out Application has authentication dependency on a local login script being executed
* Identify all places where host details (FQDN, DN, host, port etc.) are used in the Application configuration from Legacy AD Domain
* Validate if Application has Legacy AD Dependency such as Users of Application Authenticate against Legacy AD

#### Migration strategy

Where Other Application is dependent on your Application which is used to connect legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD, Application Remediation team before making changes
* Consult AD Migration team for all changes required for Application Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Validate other Application Dependency Authentication against Legacy AD and plan to make changes in all the places where AD OU Container, User Tree, Group Tree, Service Accounts, AD Groups used
* Perform the necessary testing and BCP testing.

#### Considerations

* Is there are Migration strategy
* Update the client configuration with AD details of new domain and/or server.
* Perform the necessary testing and BCP testing

## <<$No>>

* Application doesn’t have any Dependency , no change are required

# Migration Wave/s

This application come under **<<$WAVE\_NUMBER>>**  for application migration.

* The application **<<$App\_name>>** is considered part of **<<$Wave\_number>>** for the migration and planned to migrate into new domain by <**<$Date>>** tentatively.

# References

## Request for new server

* Step1
* Step2

## Request for new service/technical account

* Step1
* Step2

## Request for local share

* Step1
* Step2

## Request for **shared mailbox**

* Step1
* Step2

## Request for new DL

* Step1
* Step2

## Request for file/folder/registry permissions

* Step1
* Step2

## Support Information

|  |  |
| --- | --- |
| **Support Category** | **Contact Information** |
| Application owner | <<App\_OwnerName>> |
|  |  |
|  |  |