**Manual Migration Process**

**Contents**

[Objective: 1](#_Toc725049073)

[Step 1: Migration Process trigger – Application team 1](#_Toc1982428489)

[Step 2: Pre- Migration Checklist - Avanade 1](#_Toc41953612)

[Step 3: Encryption and data sharing 2](#_Toc512664667)

[Step 4: Recon Process 4](#_Toc357834468)

[Step 5: Encryption and sharing 5](#_Toc1734257768)

[Step 6: Signoff 6](#_Toc1733583774)

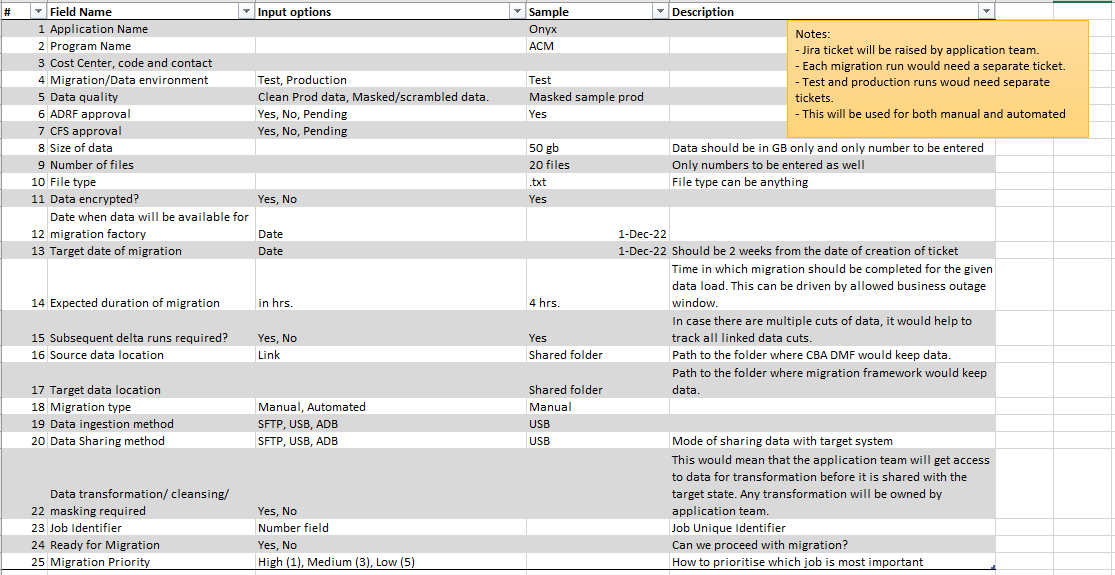
[Step 7: Offboarding Process 6](#_Toc1872241257)

# **Objective:**

The purpose of this document is to enable different application teams to move their data from CBA environment to CFS environment. This document consists of a manual process which enables the end to end migration.

# **Step 1: Migration Process trigger – Application team**

1. Application team will complete the parameter file below



1. ADM team will pick up and assign to Katherine for review and approval.
2. Once the completed file is approved, it will be “Ready for migration” and shared with Avanade team via email to start the migration process.

# **Step 2: Pre- Migration Checklist - Avanade**

**Step 2.1: Storage account**

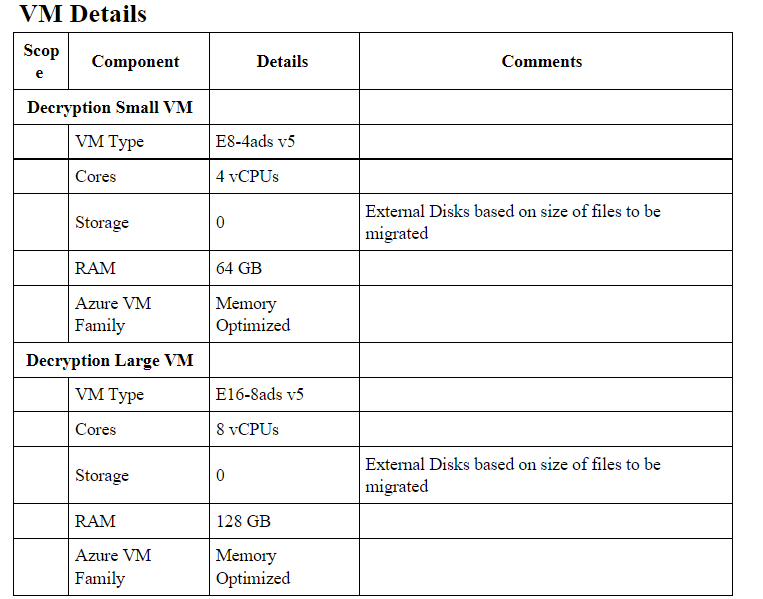
* Infra team will create the source storage account

**Step 2.2: Spin Up VM**

* Manual Engineers will reach out to Infra/DevOps team (e.g. Achroo/Rhoda) to spin up a VM using the details below: (fill it out using parameter file above)

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Columns** | **Value** | **Description** |
| 1 | Size of File to be Migrated (in TB) |  | e.g 10, 2 or 30 |
| 2 | Target (internal or external) |  | internal will be datalake, external will be sFtp |
| 3 | Owner |  | Tags |
| 4 | appName |  |
| 5 | costCenterCode |  |
| 6 | vendorName |  | For external |
| 7 | IP to be whitelisted |  | For external |
| 8 | By when we need infra Ready |  | Creation Date |

* Infra team will spin VM (see below), Disks and Destination storge account using Devops pipeline



* Infra team will provide name of Destination StorageAccount, VM name and credentials to Manual Engineers
* Infra team will share VM login credentials with Manual Engineers

# **Step 3: Encryption and data sharing**

Data sharing can happen using any of the two methods below:

**A) Azure data box management process**

**Step 3A.1: CFS**

* Make sure that subscription is enabled for Azure Data Box service. To enable the subscription for this service, [Sign up for the service](https://aka.ms/azuredataboxfromdiskdocs).
* **Sign in to Azure Portal** at <https://aka.ms/azuredataboxfromdiskdocs>.
* Create a new Azure Data Box resource in the Azure portal.
* Select a subscription enabled for this service and choose transfer type as **Import**. Provide the **Source country** where the data resides and **Azure destination region** for the data transfer. **Please specify the storage account where you wish for the data to be transferred**
* Select **Data Box Disk**. The maximum solution capacity is 35 TB and you can create multiple disk orders for larger data sizes.
* Enter the order details and shipping information. If the service is available in your region, provide notification email addresses, review the summary, and then create the order. Once the order is created, the disks are prepared for shipment.

**Step 3A.2: CBA-DMF and Microsoft**

* The data box gets shipped to CBA
* CBA will unlock the data box disk (Refer to “Connect and Unlock section” in [Quickstart for Microsoft Azure Data Box Disk | Microsoft Learn)](https://learn.microsoft.com/en-gb/azure/databox/data-box-disk-quickstart-portal?tabs=azure-portal)
* CBA encrypts files in zip format and places them in Azure databox (Refer to “copy data and validate section” for [Quickstart for Microsoft Azure Data Box Disk | Microsoft Learn”](https://learn.microsoft.com/en-gb/azure/databox/data-box-disk-quickstart-portal?tabs=azure-portal)
* Please provide manifest file to validate the contents of the data. This will be an excel file.
* Microsoft extracts data from Azure databox after connecting to Azure data center network. The data databox notifies you that data copy is complete via Azure portal.

**Step 3A.3: Application team**

* Log into the storage account specified in Task 1
* Verify that your data is in the storage account

**Step 3A.4: CBA/CFS**

* CBA provides encryption key to CFS to decrypt data via email
* CFS upload encryption key to Azure key vault.

**Step 3B.5: Avanade**

Copy the data from Landing Zone Storage to Staging Azure Storage (Managed disk) by running the script below in git hub:

Graphical user interface, text, application, email

Description automatically generated

**Please connect with Powershell team for any issues.**

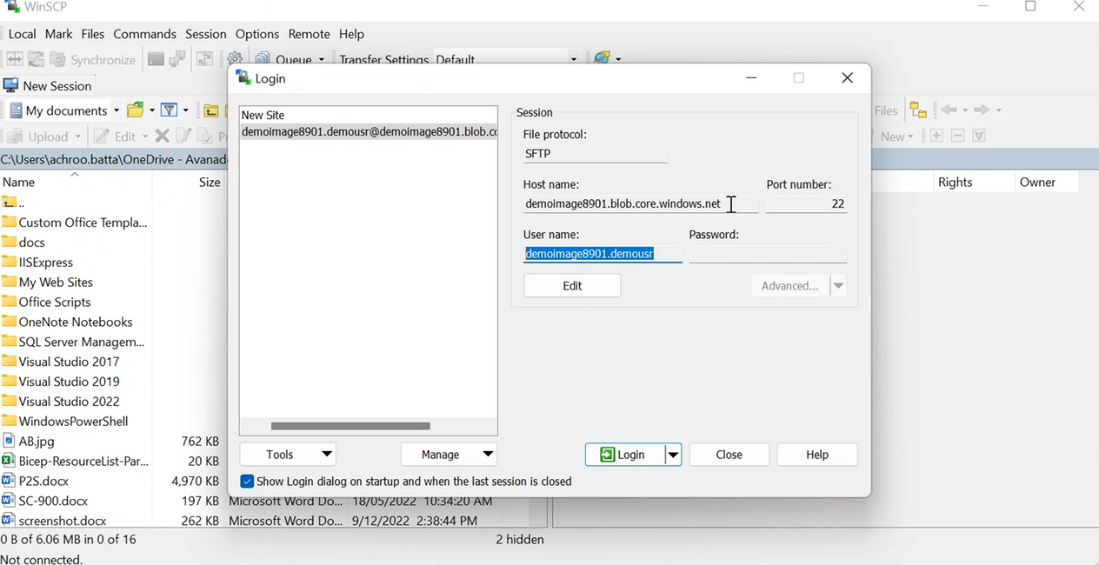
**B) CBA SFTP server**

**Step 3B.1: Avanade**

Powershell team will download WinScp application for windows

**Step 3B.2: Avanade**

Powershell team will fill out the details as seen in screenshot below



Once they click Connect, a connection is established, and the files can be dragged and dropped.

# **Step 4: Recon Process**

Once the data has arrived using any of the methods above, proceed with the recon process:

1) Files are copied from storage account to managed disk 1 where they are kept as a read only copy. Use Z drive to copy zipped files and U drive to copy unzipped files.

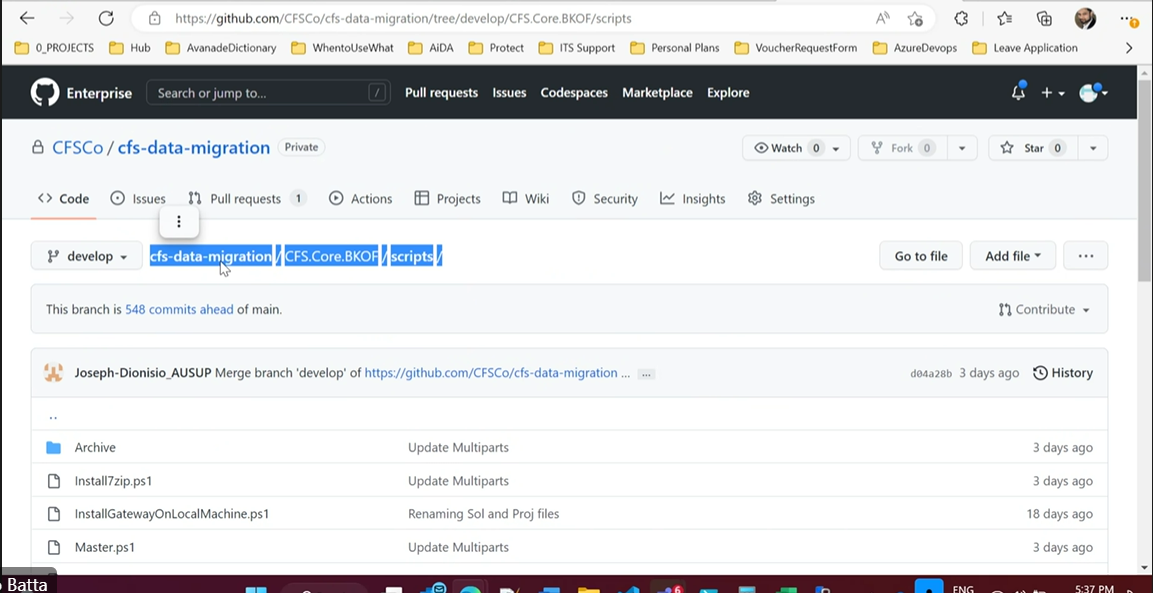
2) Files are copied from managed disk 1 (Z drive) to managed disk 2 (U drive). Files are decrypted in U drive using 7zip using the encryption key from Azure Key Vault.

3) Once files are decrypted, Microsoft defender is run to ensure no malware is present.

4) Engineers will conduct recon process manually. They will manually validate the following items:

* Validate total number of files and folders – **Avanade to validate**
* Validate the hash of the folder or each file and ensure it matches the source hash – **Application team to validate**

**Please reach out to Power shell team to access scripts in the repository below:**



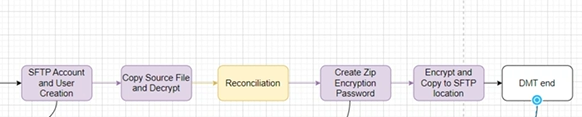
# **Step 5: Encryption and sharing**

**Internal sharing: Application team**

* The files will not be encrypted within the environment
* Data will be available unzipped on VM. It’s up to the application team to decide what to do with it.

**External sharing: Avanade**

1. Infra team will create sftp account and create user details with SSH key.
2. Manual Engineers will generate zip encryption password using the script in github library and store it in key vault. **(Reach out to power shell team to get script details).**
3. Manual engineer will re-encrypt the files with above password and copy to SFTP blob storage location created by Infra team using script.
4. Manual engineers share SSH key and password to application team via email
5. Application team will share the above details with 3rd party user using above details.
6. Application team confirms with 3rd party user that they can access data
7. 3rd party user can access the files in the SFTP blob storage account for external use **(Reference: Low Level Design - External access path)**



# **Step 6: Signoff**

* CFS team to verify that the data has reached target state (storage accounts) for external use and azure blob storage for internal use

# **Step 7: Offboarding Process**

* After migration is completed, data needs to be retained from 1-6 months as specified in the parameter file earlier.
* If the migration fails, CFS will come up with a plan to either rollback or retry migration.
* CFS team to verify that the data has reached target state (storage accounts) for external use and azure blob storage for internal use
* Once migration is completed, small and large VMs that are not longer required will be deleted.
* Once data is onboarded, Application team will conduct Functional testing during the warranty period specified by Risk team
* Once functional testing is completed, get signoff from Application team and Avanade team to delete the data.

**Attached is a RACI matrix for the above process addressing additional tasks and roles/responsibilities:**



**Considerations:**

* This process is highly manual and requires workarounds
* CFS is responsible for making sure the excel migration template shared with Avanade is completed, doesn’t contain duplicate information, has all the mandatory fields, is not corrupted and is signed off before migration is executed
* In case of any duplication, Avanade team will raise it with CFS team immediately and they will action it
* CFS will provide guidance on which migration requests need to be actioned first

**Reference document:**

|  |  |  |
| --- | --- | --- |
| **Sr#** | **Reference Document** | **Description** |
| 1 | [Migration Landing Zone and Decryption SOAP - CFS IT - Confluence (prod.cba)](https://confluence.prod.cba/display/CFSIT/Migration+Landing+Zone+and+Decryption+SOAP) | HL SOAP for migration generic components |
| 2 | Migration Landing Zone – Low Level Design | Design Document |