Cognizant Microsoft Business Group

Azure Migration Guide

Presented to:

Noble Drilling Corp.

3/19/2021

Cognizant Microsoft Business Group
20 North Wacker Drive #530
Chicago, IL 60606

TABLE OF CONTENTS

SUMMARY

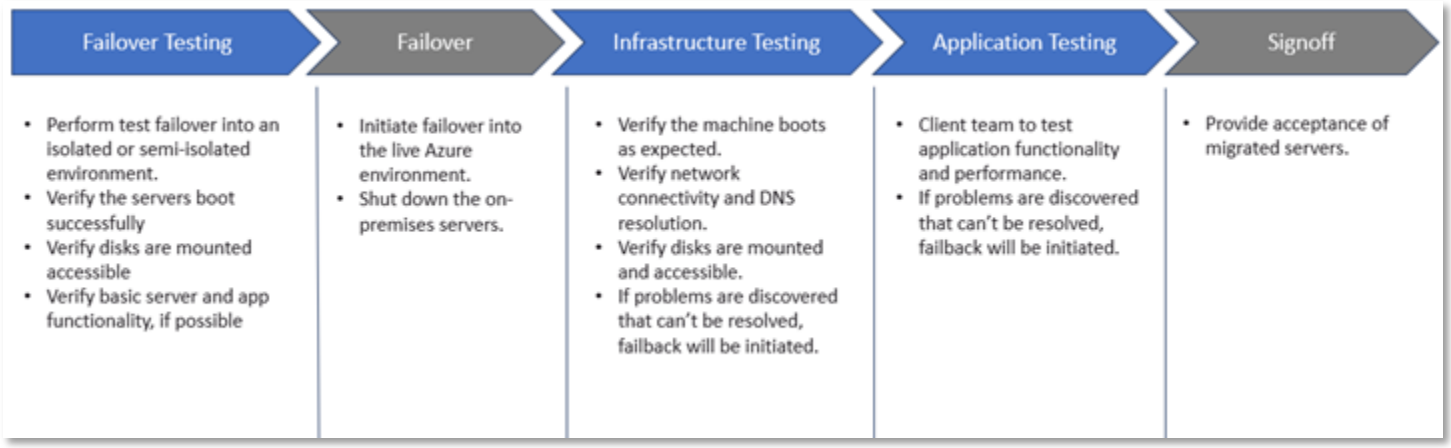
This document is intended to provide guidance for migrations to Azure along with testing before and after rehosting of a server or workload to Azure. It is important to perform testing on workloads moving to the cloud to verify:

- Migration tooling functionality
- Proper bandwidth and network connectivity
- Verify right sizing to ensure acceptable performance level is still being achieved in Azure
- Verify any established benchmarks are being met in Azure
- Verify no compatibility issues exist that may have been previously unaccounted for

There are three types of testing that should be performed during the migration lifecycle:

1. Failover testing - this testing takes place before migration to ensure the failover to Azure happens with as little interruption in service as possible. This could be as short as verifying the VM boots, to as much as fully testing an application in an isolated environment in Azure.
2. Virtual infrastructure testing - this testing takes place after failover and ensures the VMs and Azure virtual infrastructure are all configured and performing as expected.
3. Application testing - this testing will be performed by the application teams that understand the workload that has been migrated. This testing should be a full QA test of the workload to ensure that it is performing as expected and suitable to continue as production.

Workload Migration Lifecycle

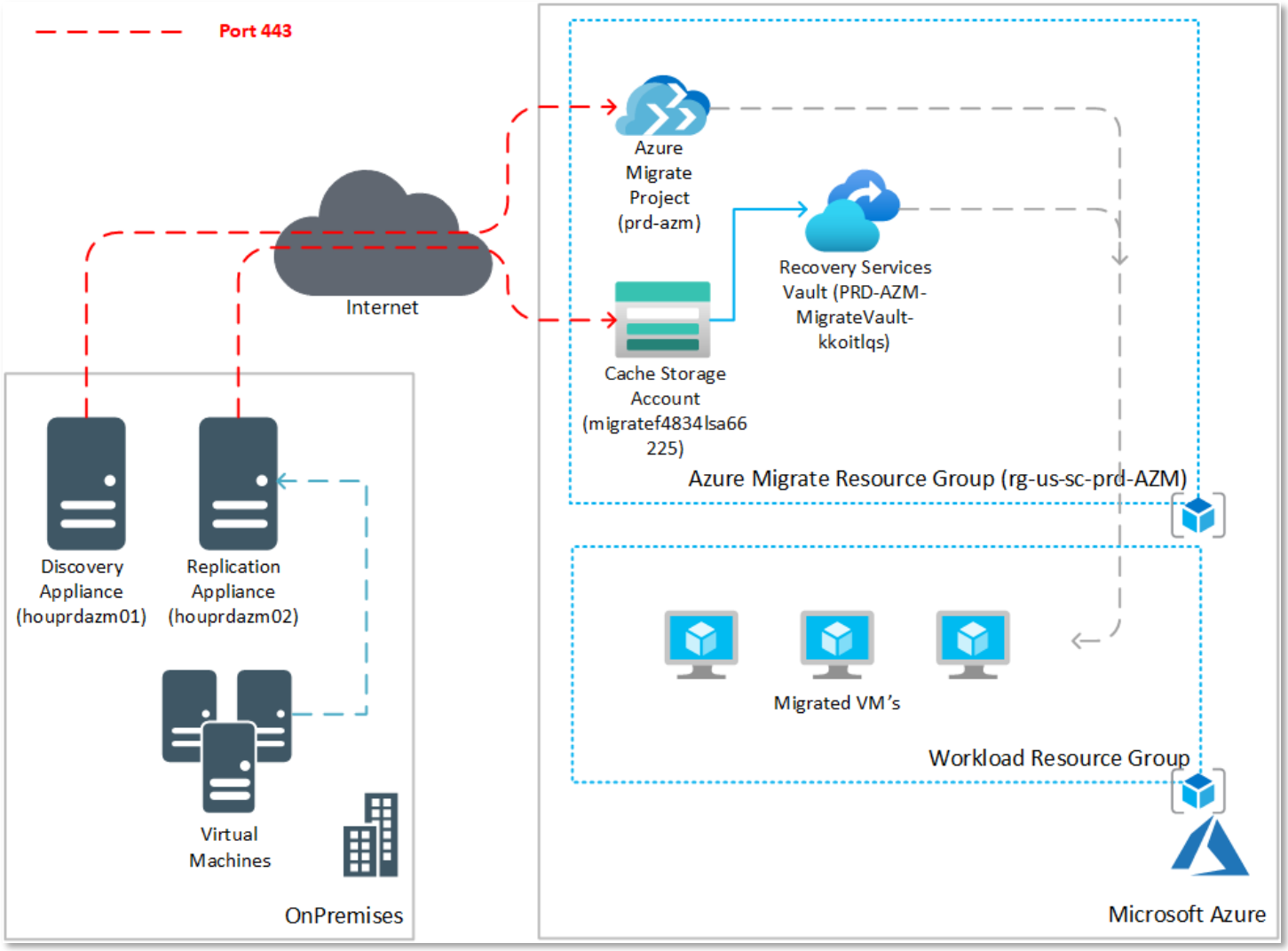


DEPLOYMENT CONSIDERATIONS

- When replicating a physical server (non-VMware or Hyper-V virtual machines included), the assessment portion of Azure Migrate will not interact with the migration tooling.
- Each migration project will be limited to one region (one-to-one relationship), to replicate to multiple regions one Azure Migrate project and Configuration/Process server will need to be created.

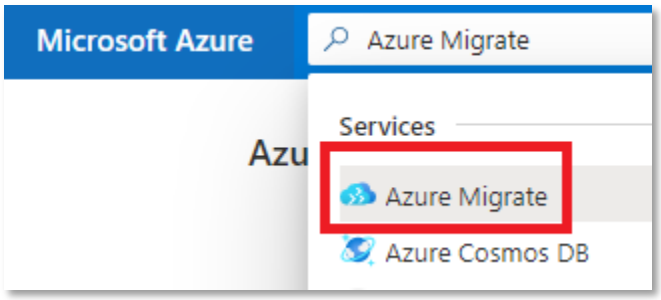
CURRENT DEPLOYMENT TOPOLOGY

Below is the current topology for Noble, The Discovery Appliance is performing sizing and dependency mappings of virtual machines and the Replication Appliance is replicating selected virtual machines using the Mobility Agent installed on each server into the Azure Migrate Project via the Cache Storage account and storing that data within the Recovery Services Vault for failover into Azure.

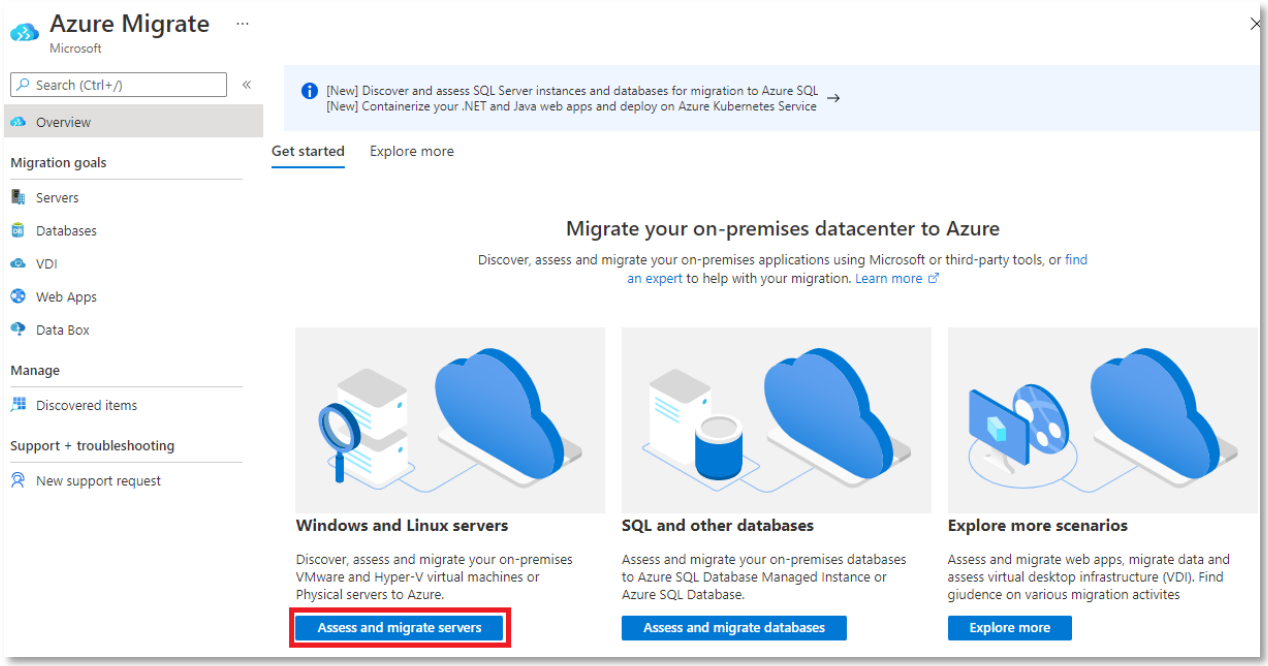


Deploy Azure Migrate project in the portal

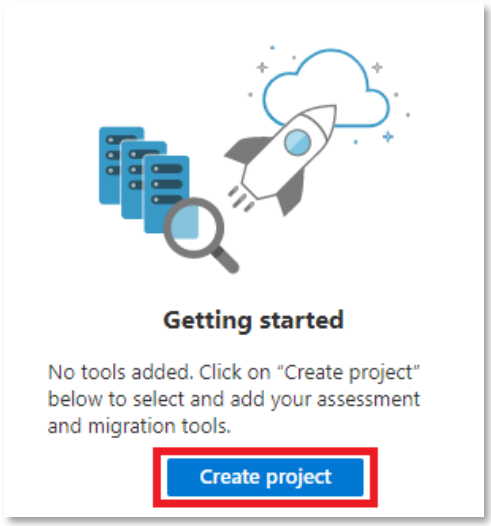
- Navigate to the Azure portal and search for Azure Migrate



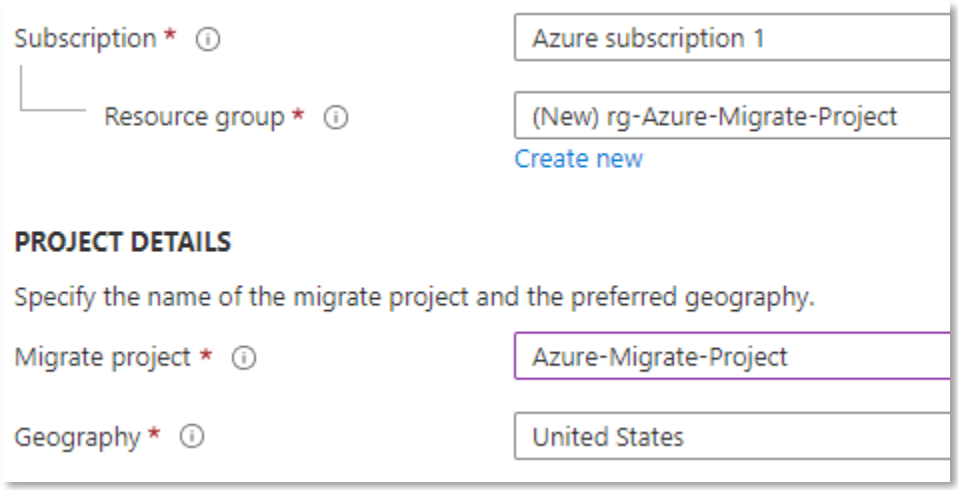
- Once on the Azure Migrate page select Asses and migrate servers



- Select create project



- Select the subscription and resource group to create the Azure Migrate project under
    - Make sure to select the proper geography for where your servers will migrate to

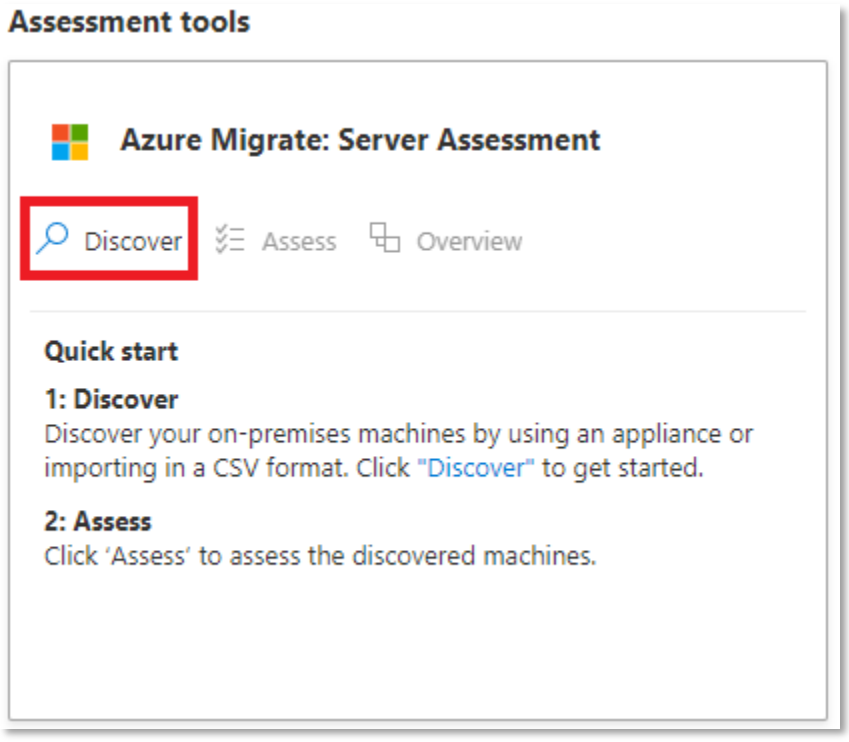


- Your project has been created and you can now begin the Assessment process.

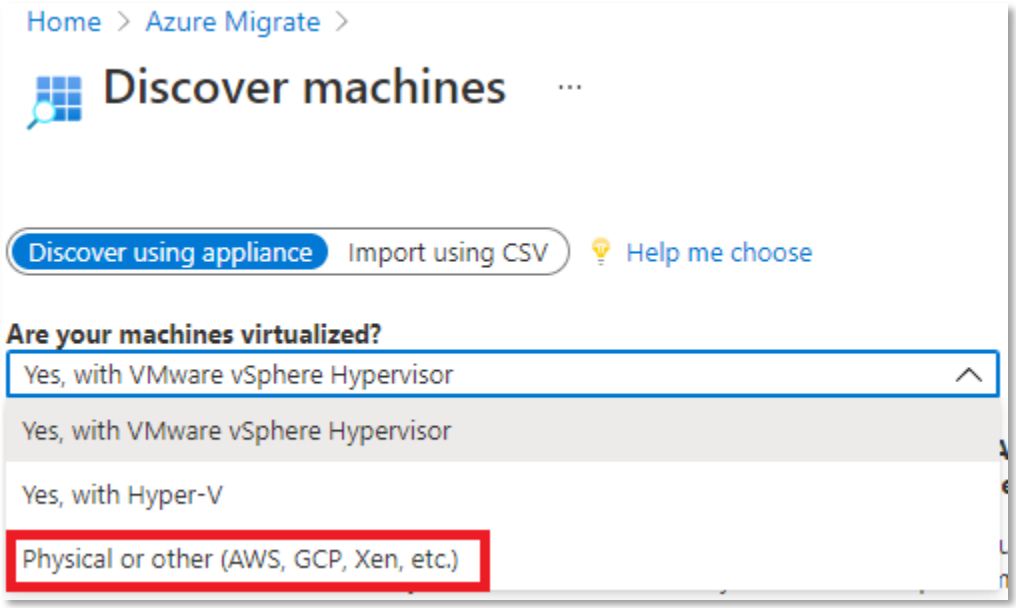
Deploy Assessment appliance server

Prerequisites: VM with Windows Server 2016, 16GB of RAM, 8 vCPUs and 80GB of storage

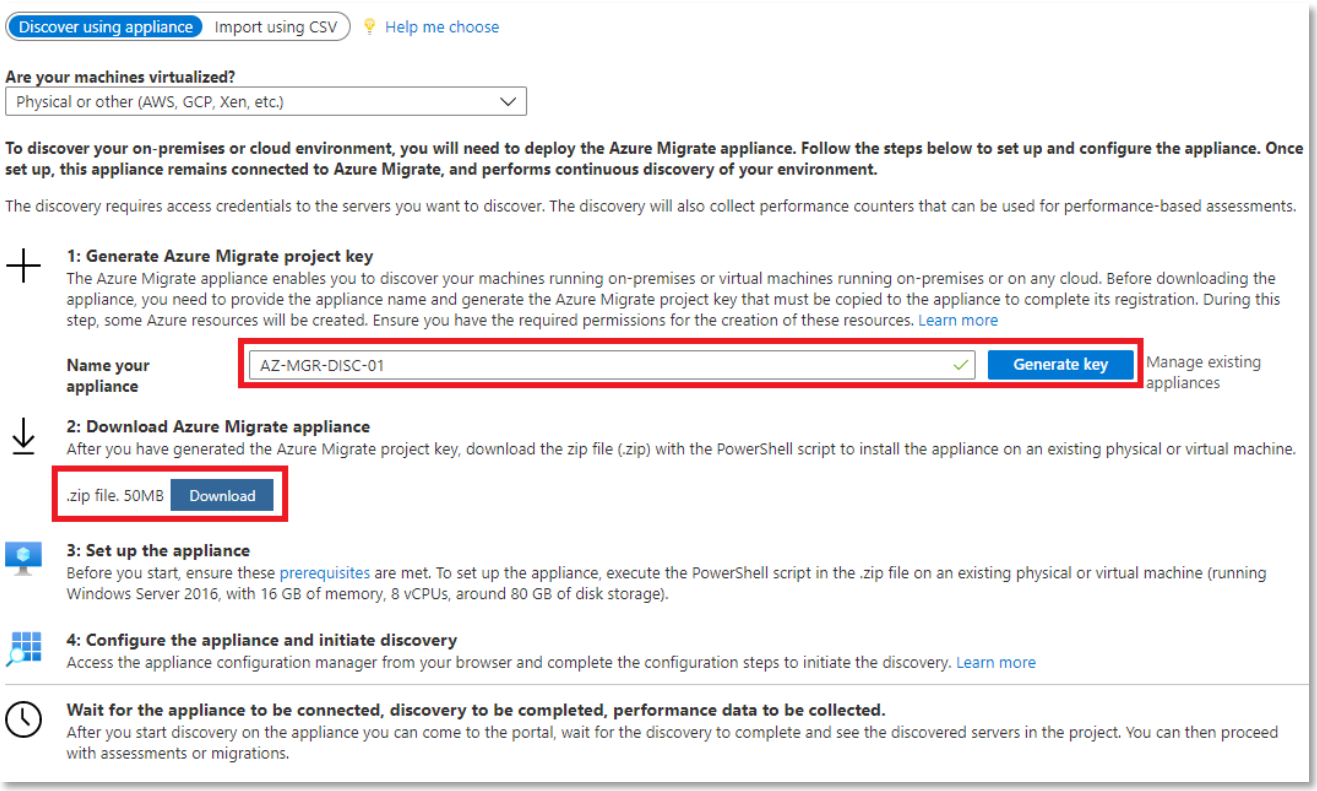
- In the Azure Migrate project select the Discover button under the Azure Migrate: Server Assessment section

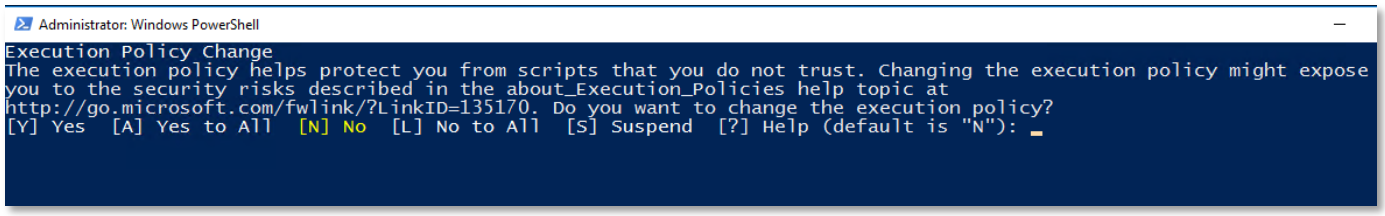


- Once on the Discover machines page open the dropdown and select Physical or other (AWS, GCP, Xen, etc.)

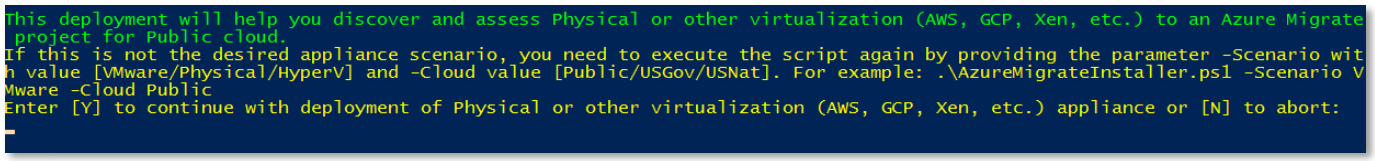


- Fill in the Name your appliance section (Make sure this matches the name of your discovery server)
- Generate your key and copy the information down.
- Download the Azure Migrate appliance zip file. Make sure to copy the zip file and key info to your appliance.

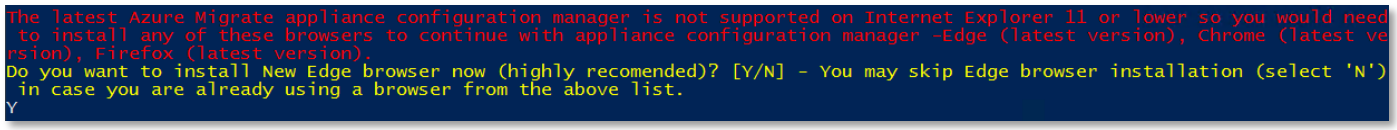


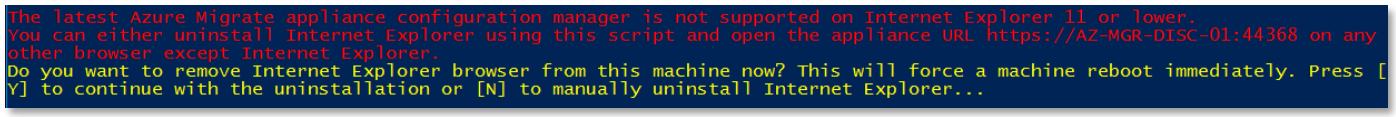
- Extract the Azure Migrate Installer .zip and run the AzureMigrateInstaller.ps1 file
- 

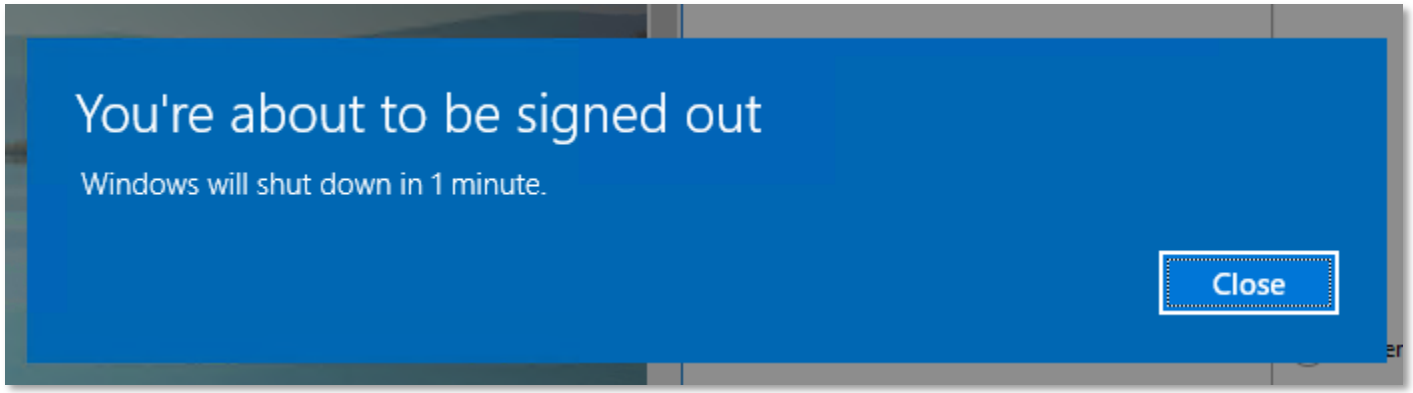
  Type A for “Yes to All”

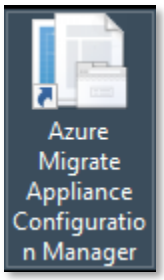
- 

  Type Y to continue

- When prompted you can install the latest version of Microsoft Edge
- 

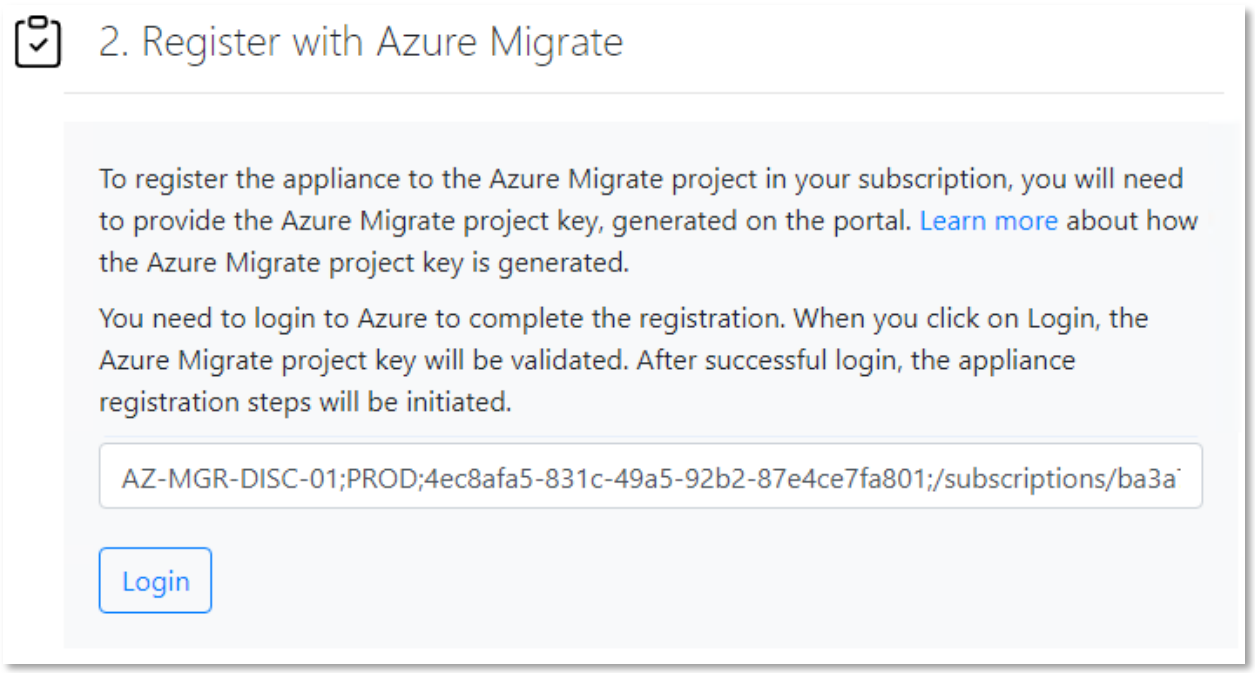
- Allow the installer to remove Internet Explorer
- 

- The installer will finish and restart the system automatically.
- 

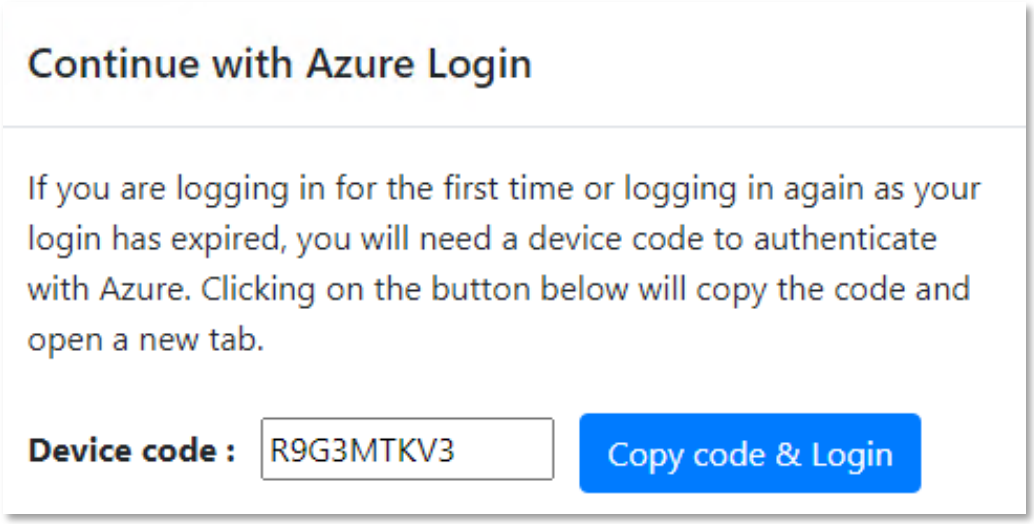
- Once the system restarts the Appliance Configuration Manager will automatically open
  - (If this does not happen you can also open the shortcut on the desktop.)
  - 

- The system will run through the prerequisites and verify the system is ready to start discovery.

- Take the key we generated in the Azure Migrate portal and enter it into the box and click Login

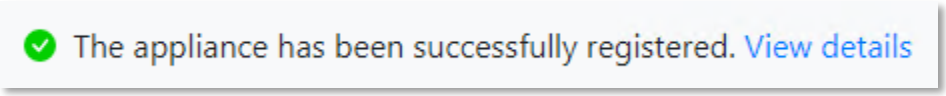


- Click on Copy code & Login to be brought to the Microsoft login page. Here we will associate the appliance using an Azure account with Administrator rights to the Azure tenant.



- Once the login is complete you will be shown this screen.

- The appliance will register with the Azure Migrate Project which can take up to 10 minutes



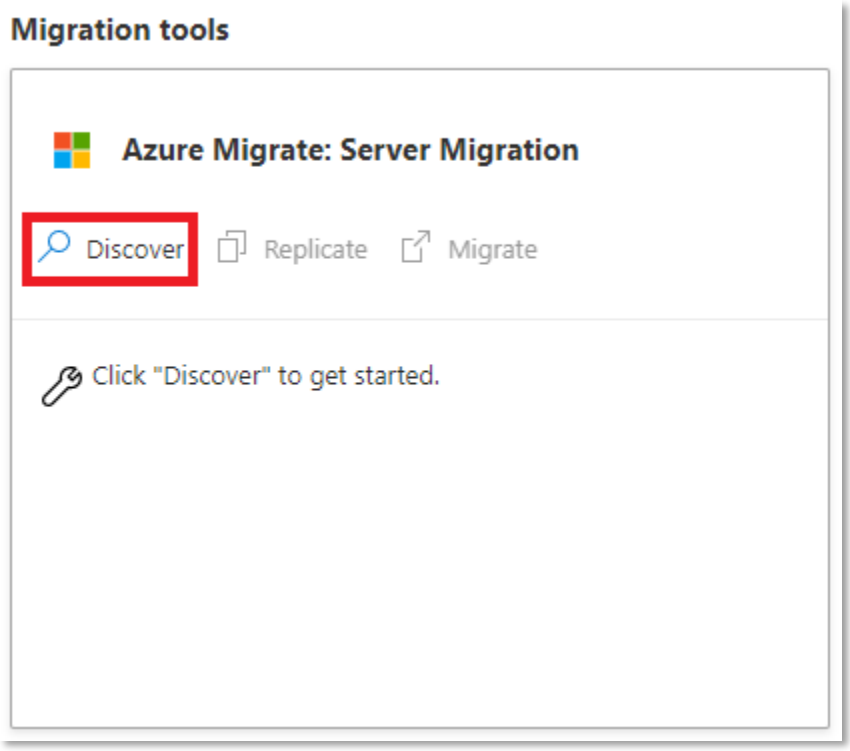
Deploy Migration appliance server

Prerequisites: VM with Windows Server 2016, 16GB of RAM, 8 vCPUs and 300GB of storage

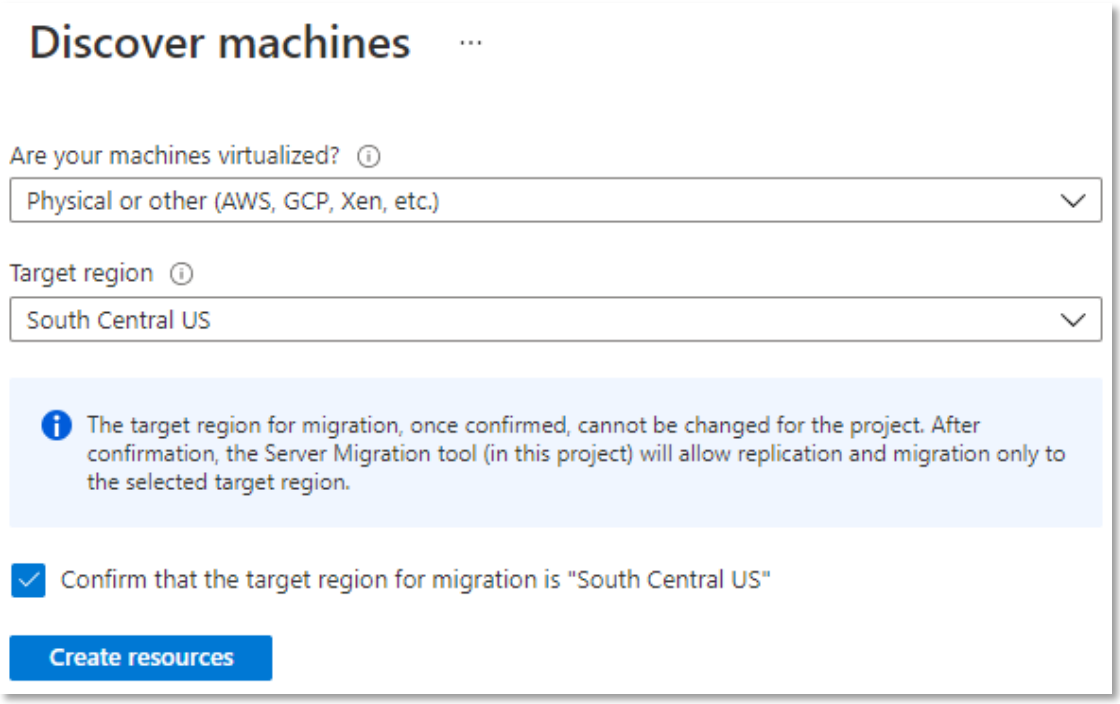
Note: The virtual machine can be provisioned with one or two vNICs for redundancy

Replication appliance detailed sizing information: [Azure Migrate Server Migration Scaling | Microsoft Docs]

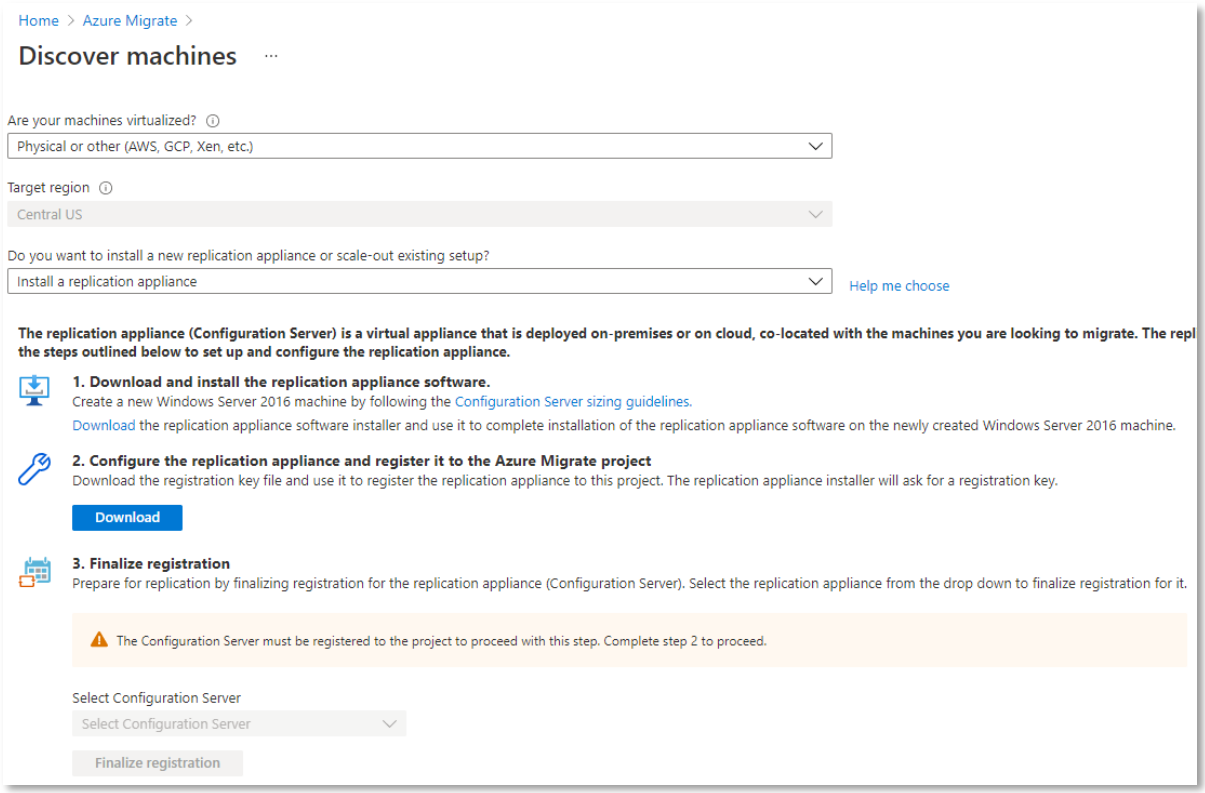
- In the Azure Migrate project select Discover under the Azure Migrate: Server Migration section



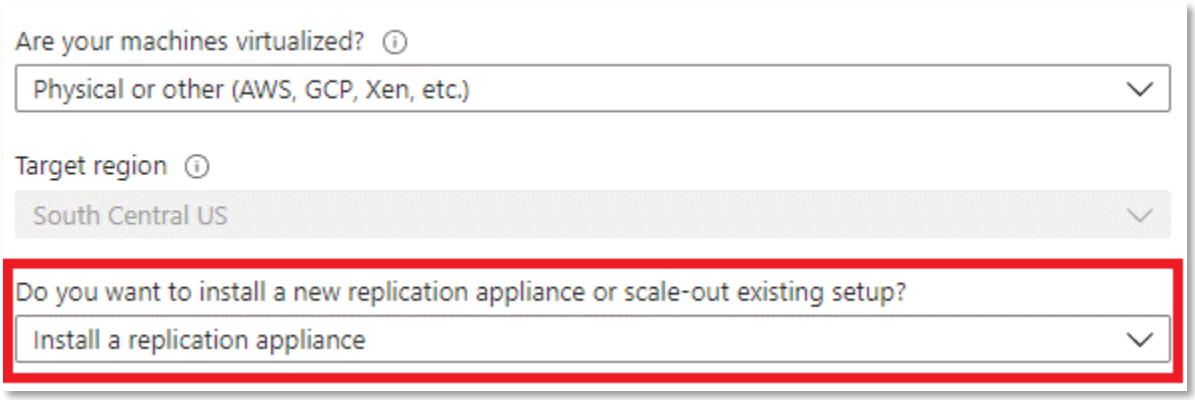
- Select Physical or other for the virtualization type and your Target migration region



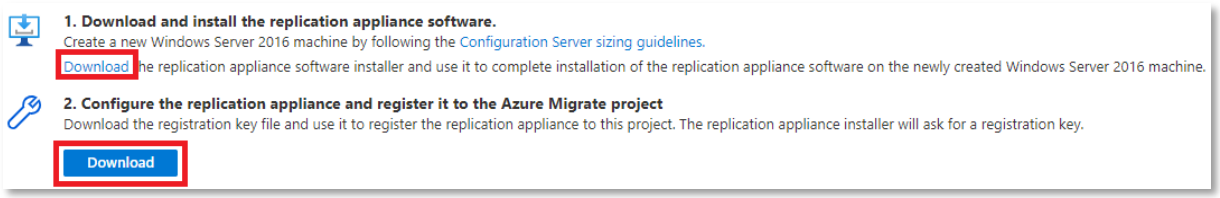
- Azure Migrate will deploy the necessary resources for you and bring you to the following screen



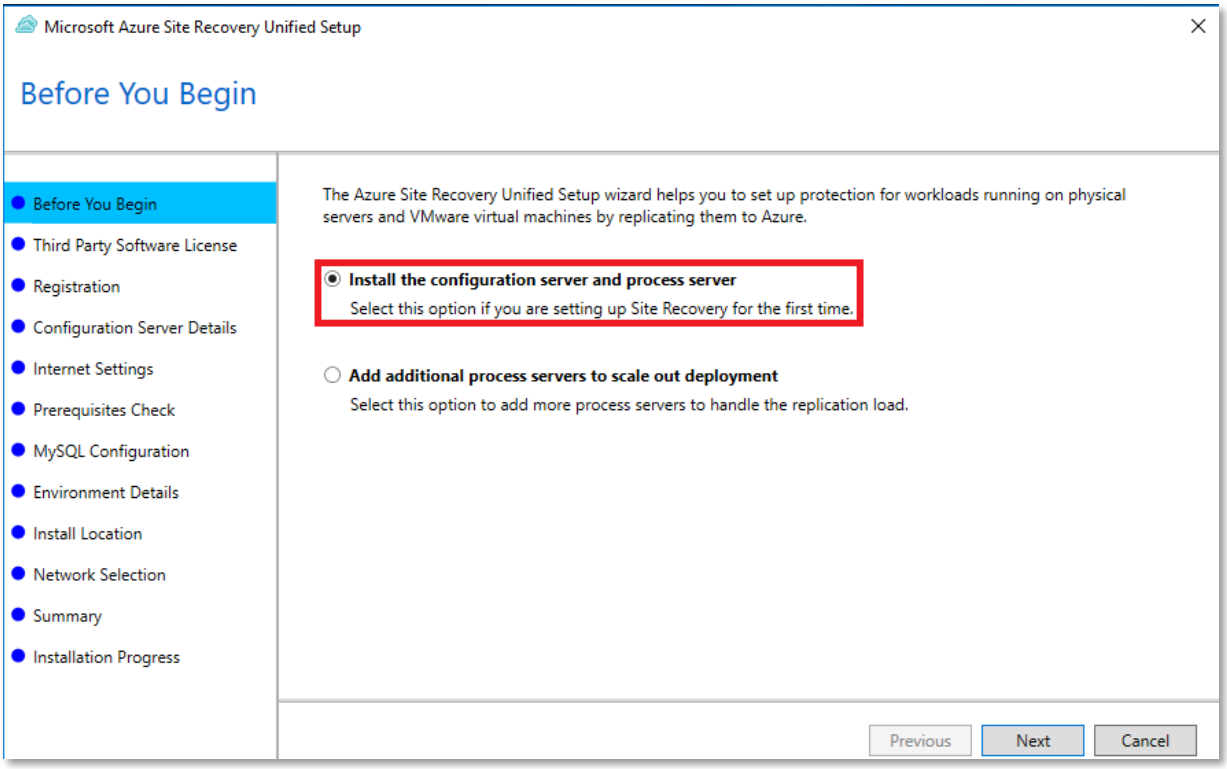
- Select Install a replication appliance in the dropdown



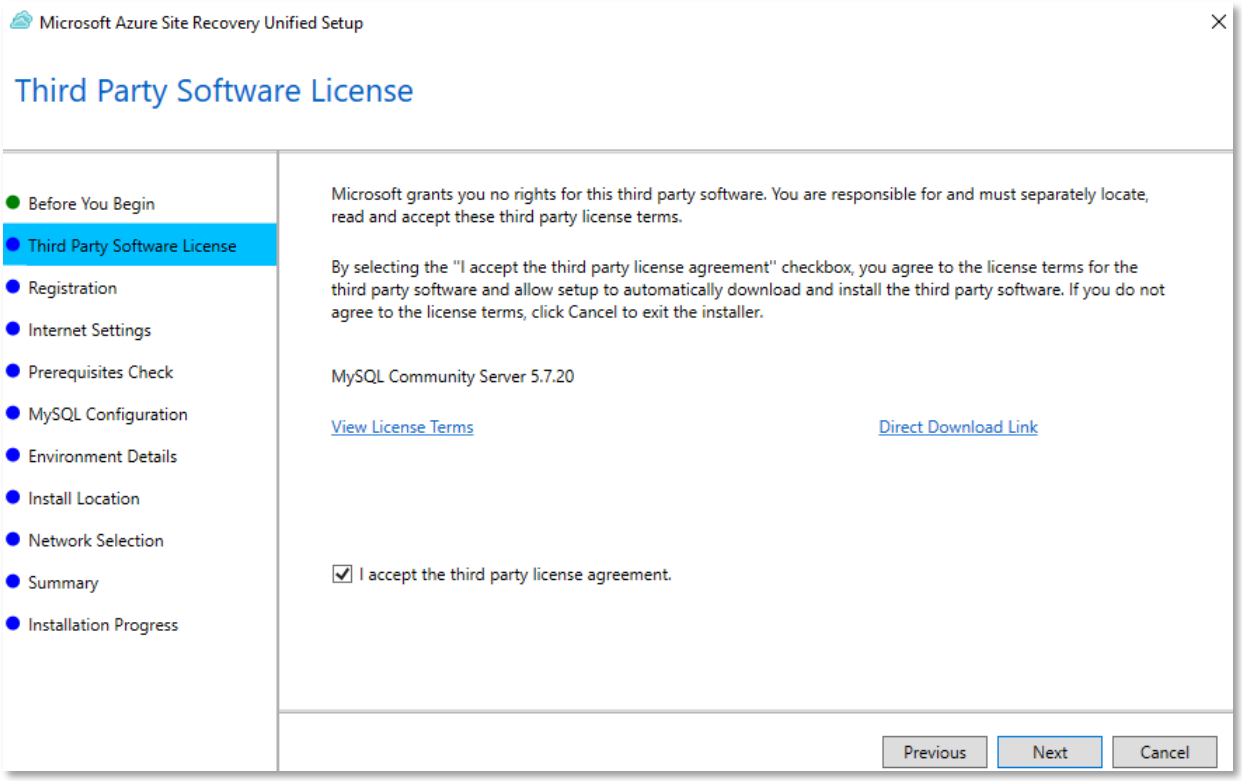
- Click the two links to download the replication appliance software and the registration key file
  - The installer is based on the target region chosen in the step above and can be downloaded from: http://aka.ms/unifiedinstaller_scus (South Central Us)



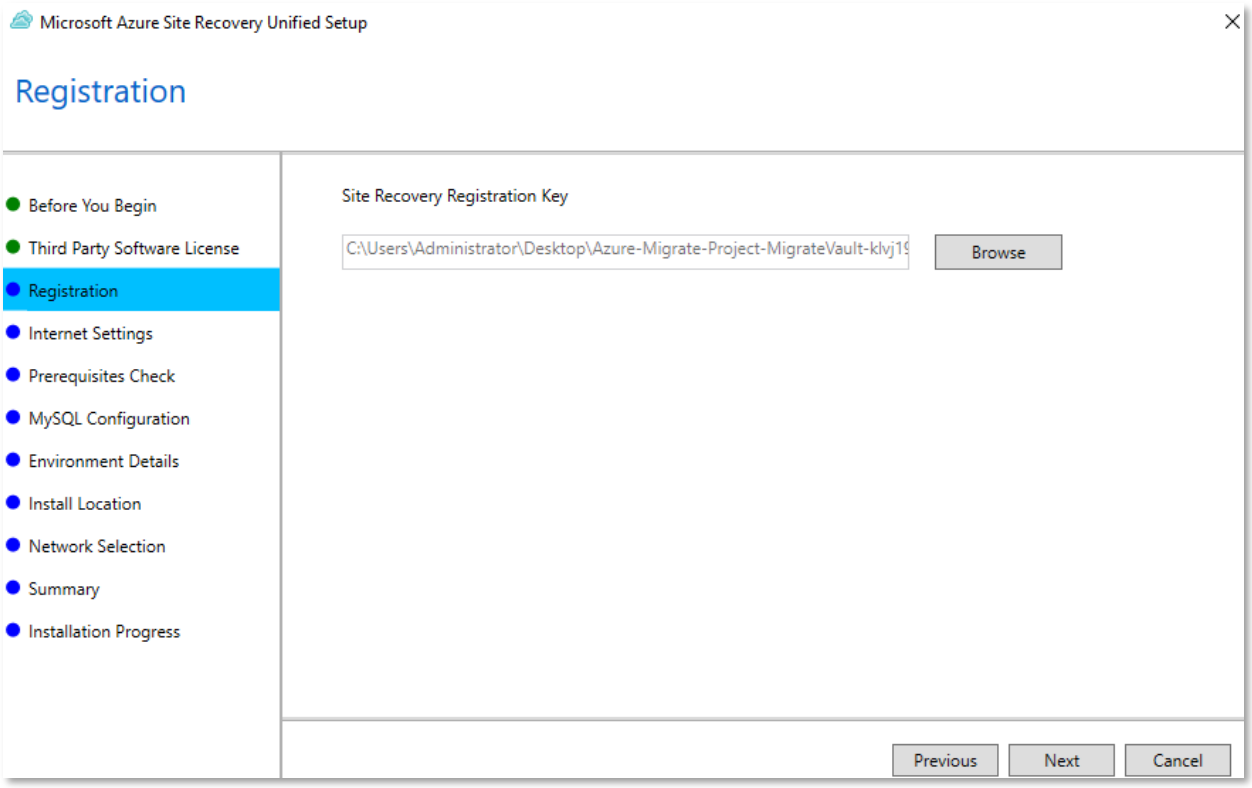
- Copy the installer and key file to your replication appliance and run the installer
    - Make sure "Install the configuration server and process server" is selected



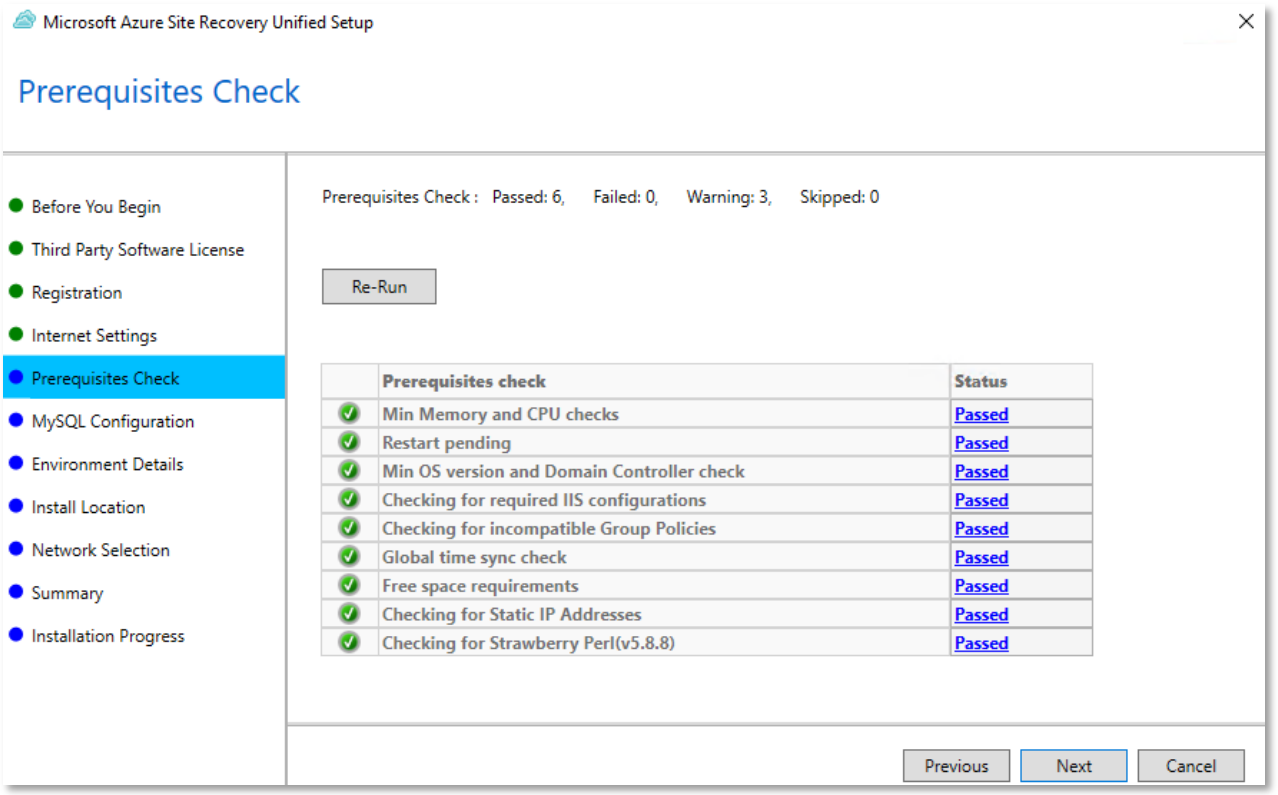
- Accept the license agreement for SQL to be installed on the appliance



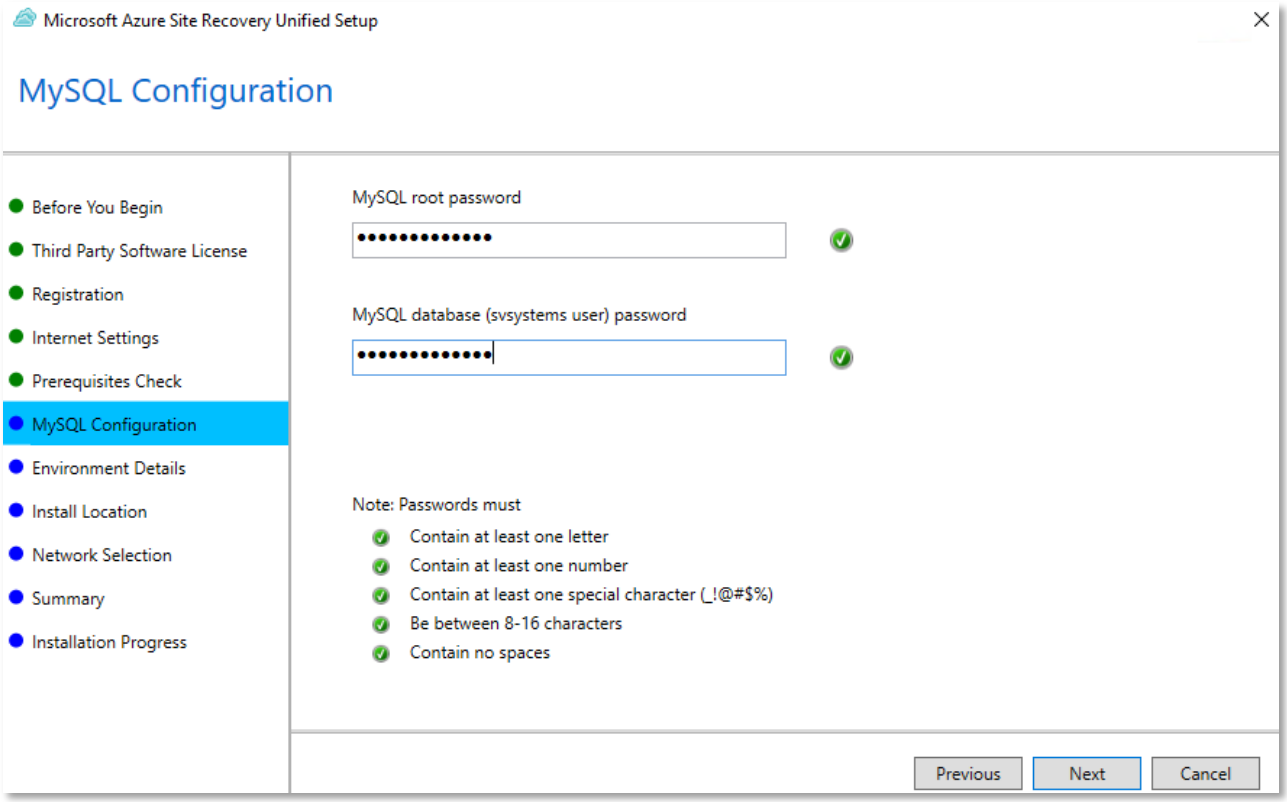
- Select your key file previously downloaded from the Azure portal



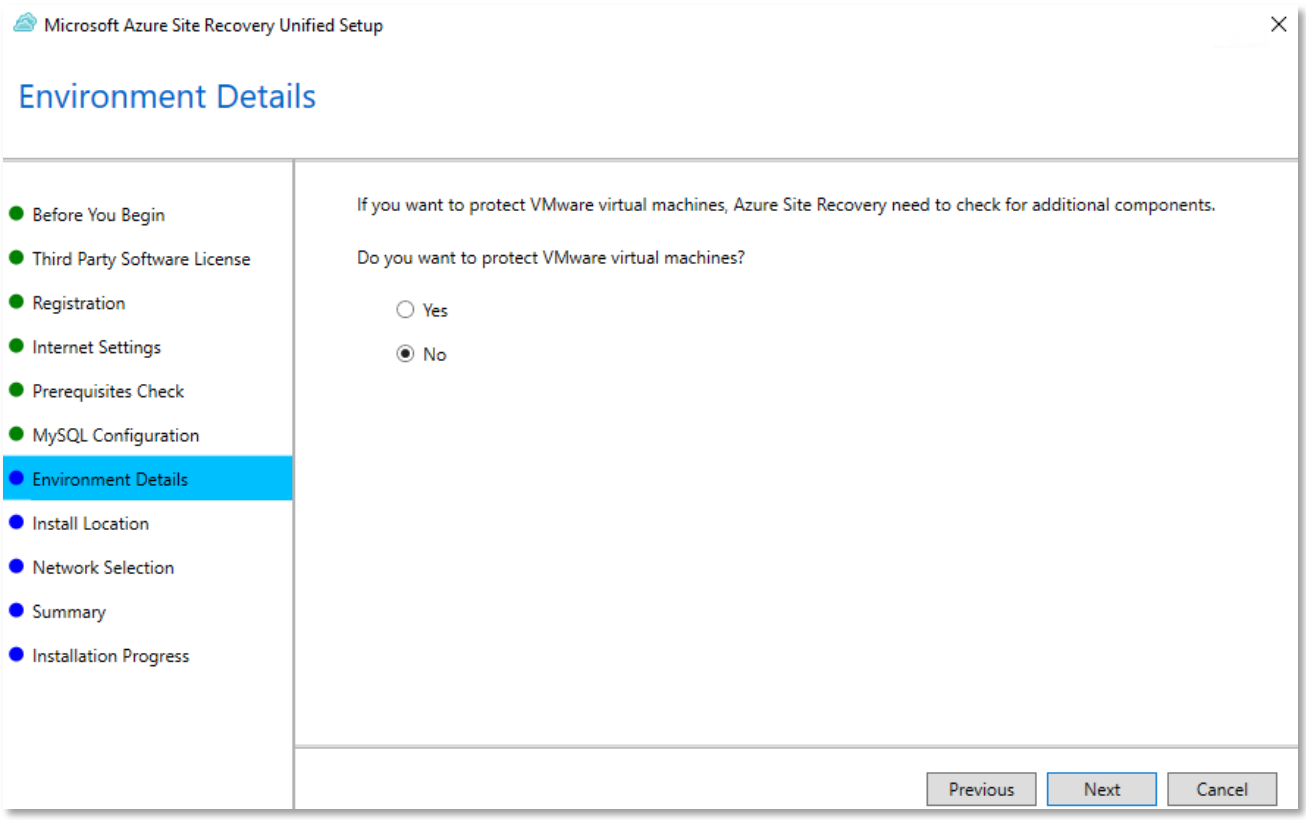
- Configure any necessary settings for connecting to Azure, the system will verify the settings once you click Next.
- The system will run through prerequisite checks and notify of any errors.



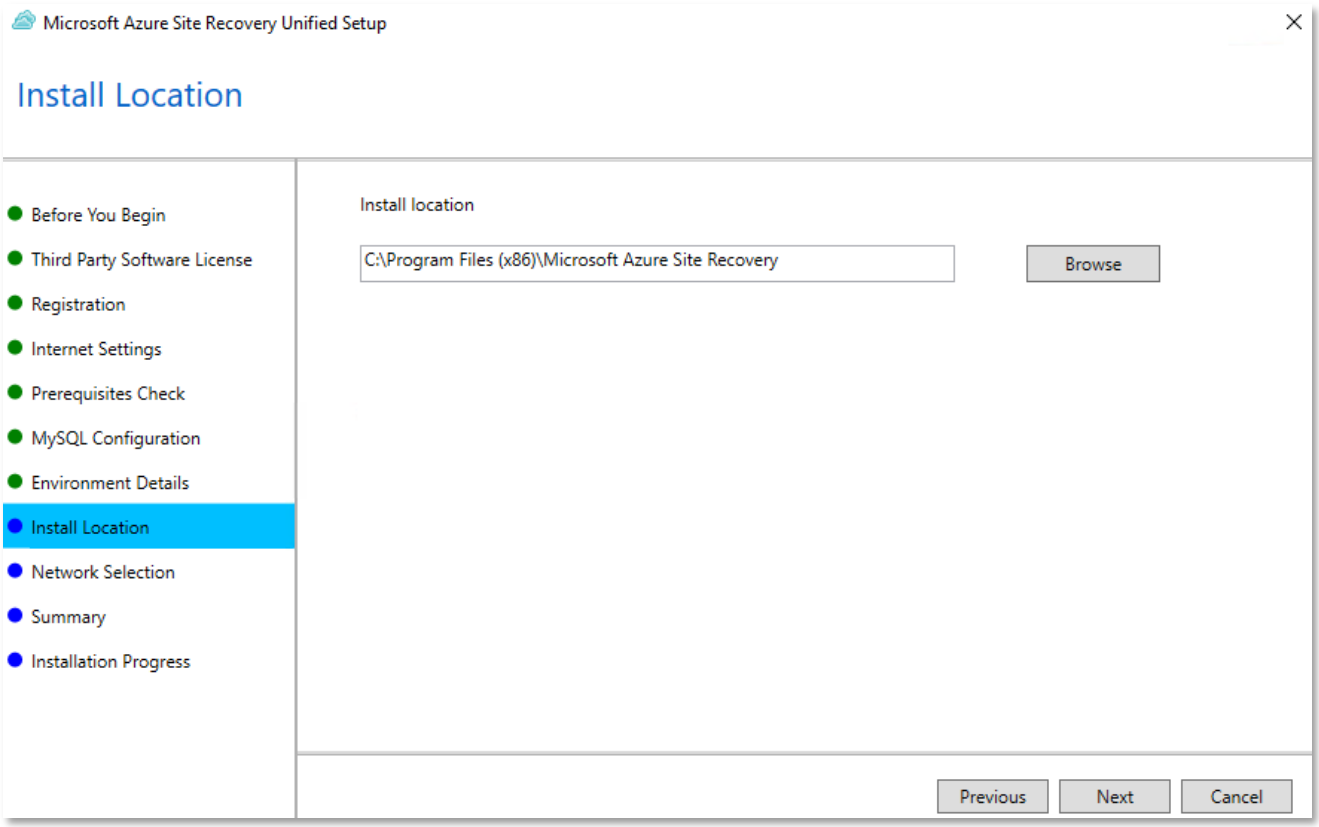
- Configure a password for the MySQL root account



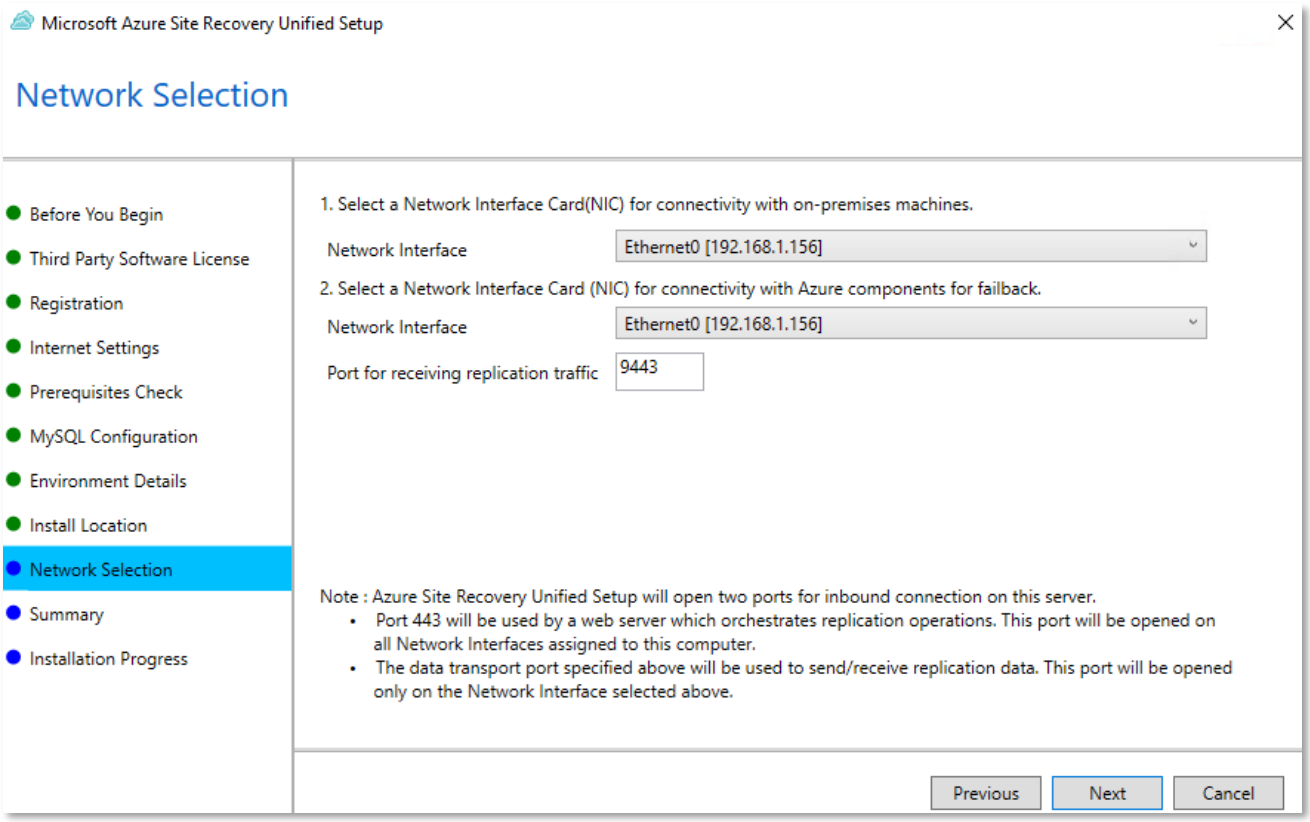
- Select No when prompted "Do you want to protect VMWare virtual machines"



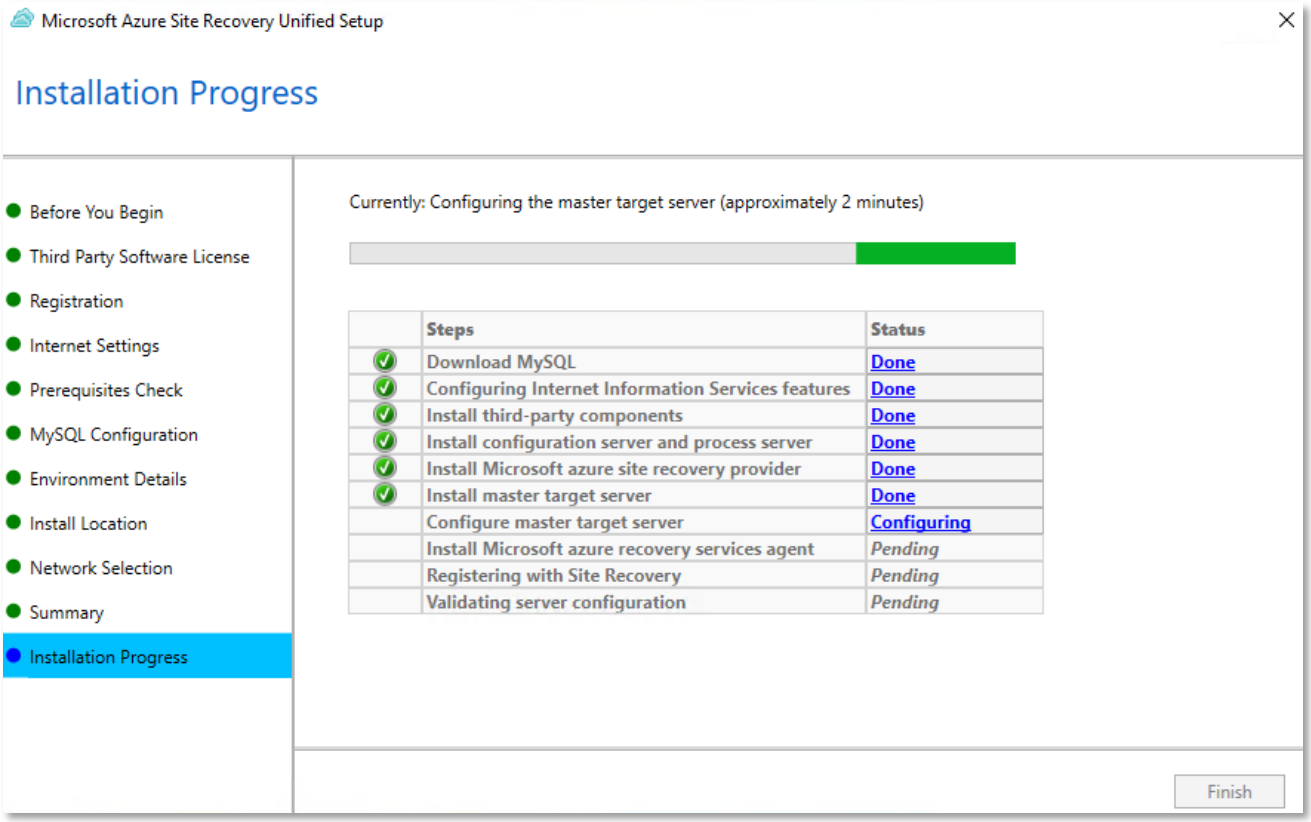
- Select your install location, make sure this is on a drive with 600GB+ of storage



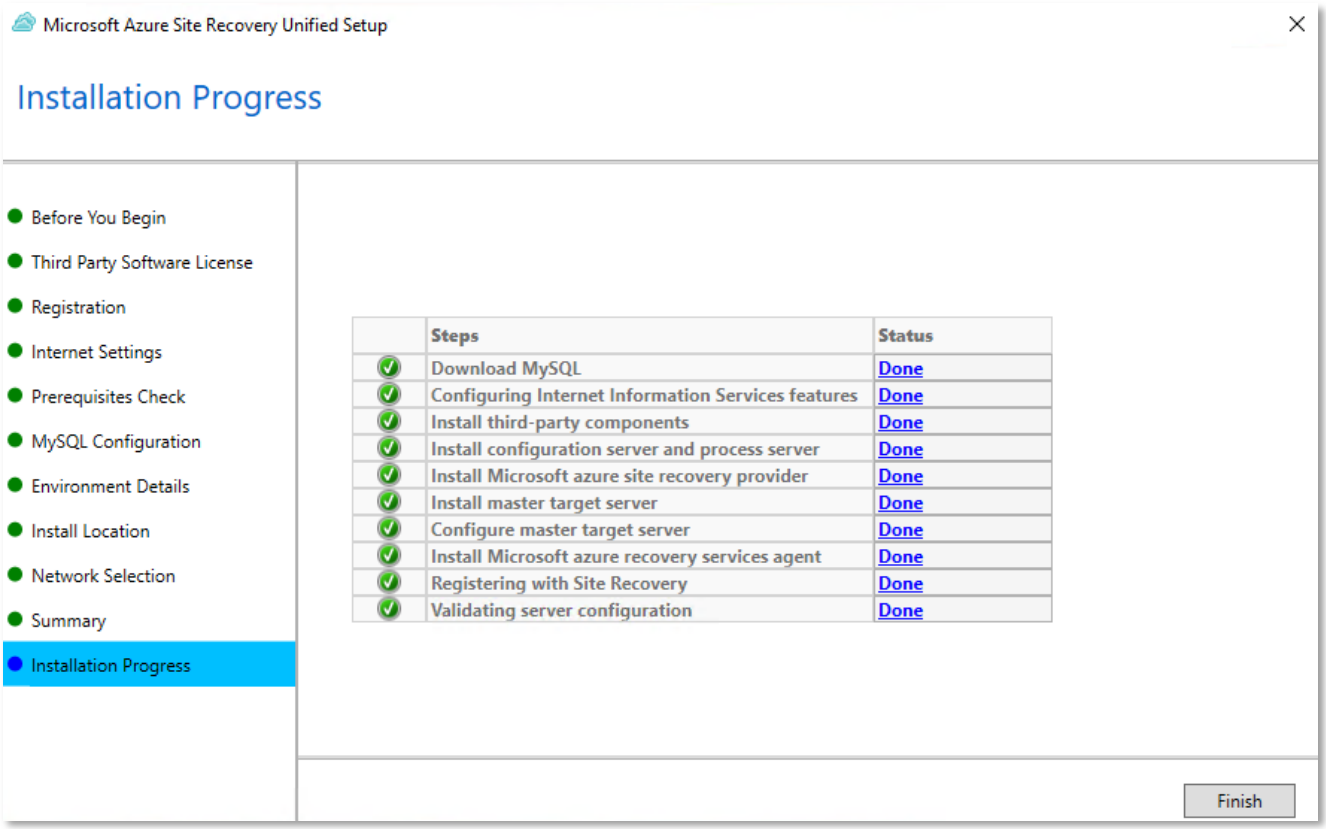
- Select the appropriate network interfaces for replication and failover



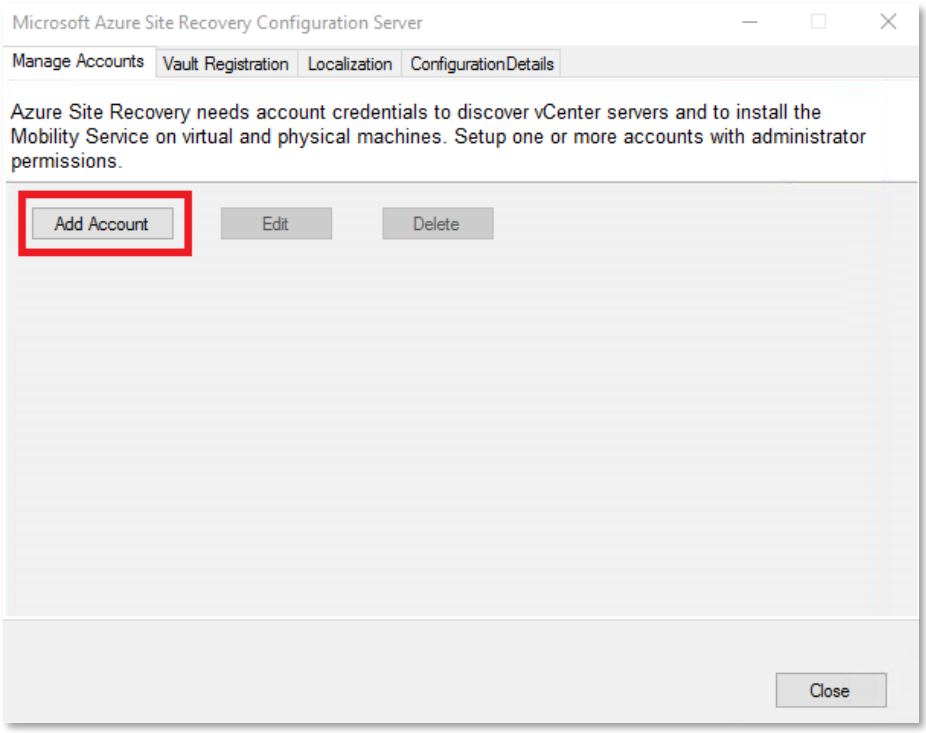
- The system will give you a summary and you can start the installation process.



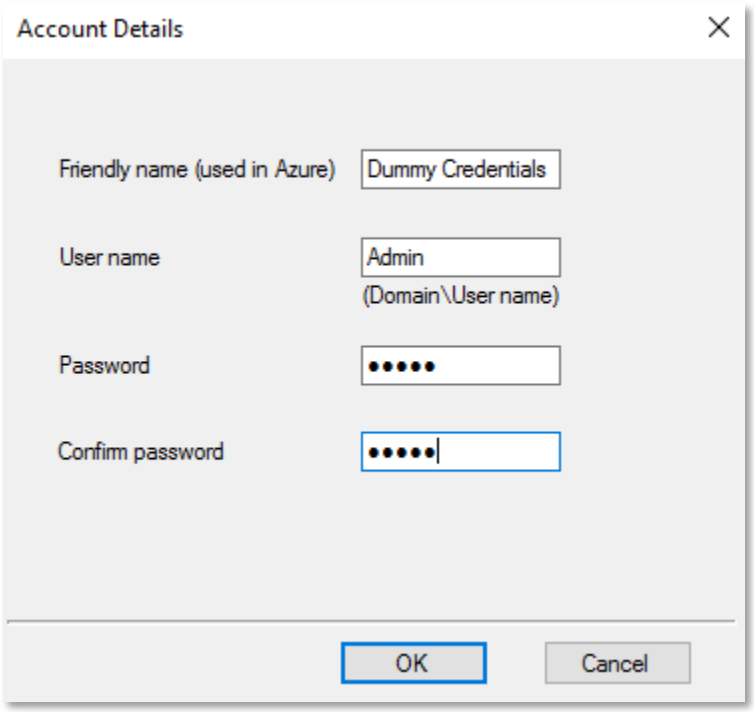
- Once the installation is complete you can click Finish to close the installer.
    - You will receive a popup with a connection passphrase, make sure to document this as it will be needed when installing the Mobility service on servers for replication.



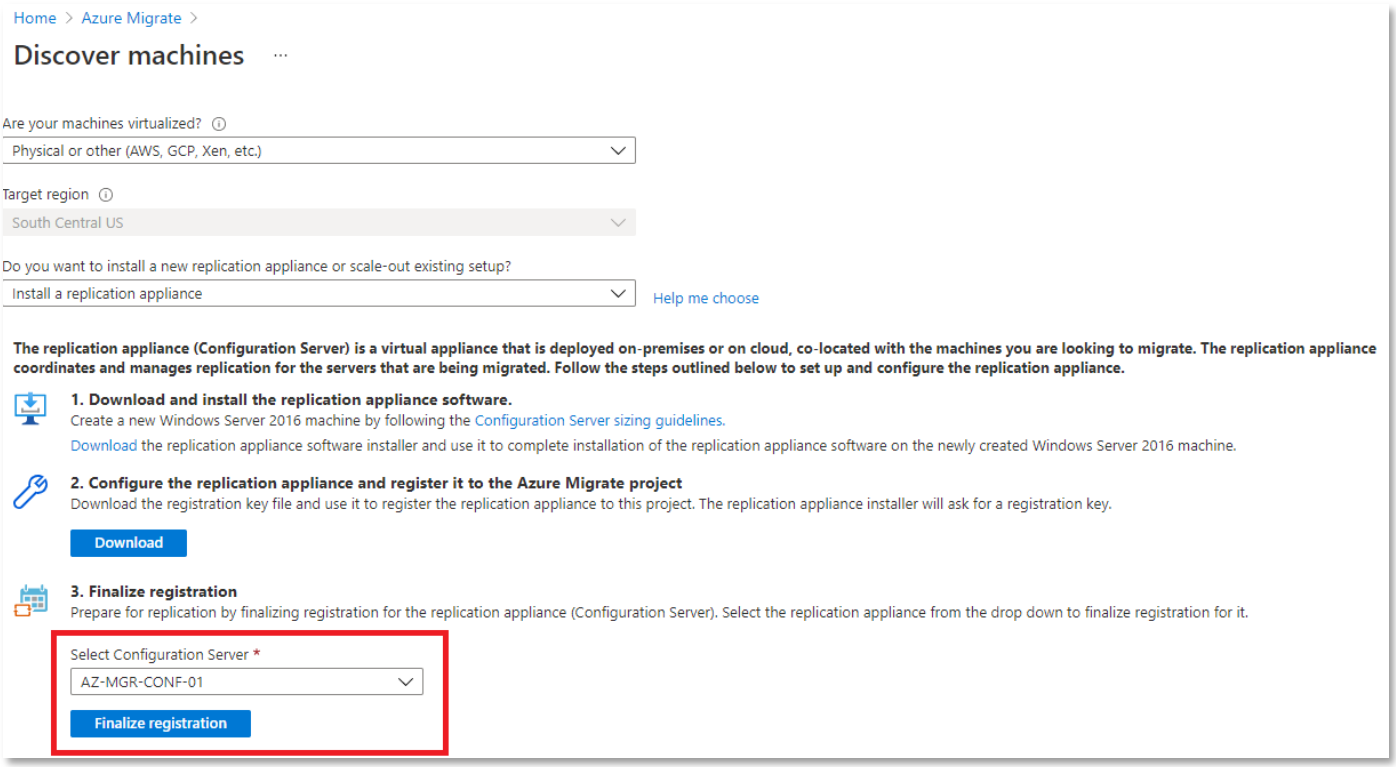
- The Microsoft Azure Site Recovery Configuration Server application will now open, click the Add Account button



- Enter a set of dummy credentials, ie. Admin for the username and password



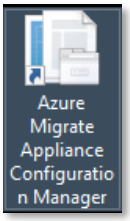
- Navigate back to the Azure Migrate portal
    - Select your configuration server under Finalize Registration and click Finalize registration



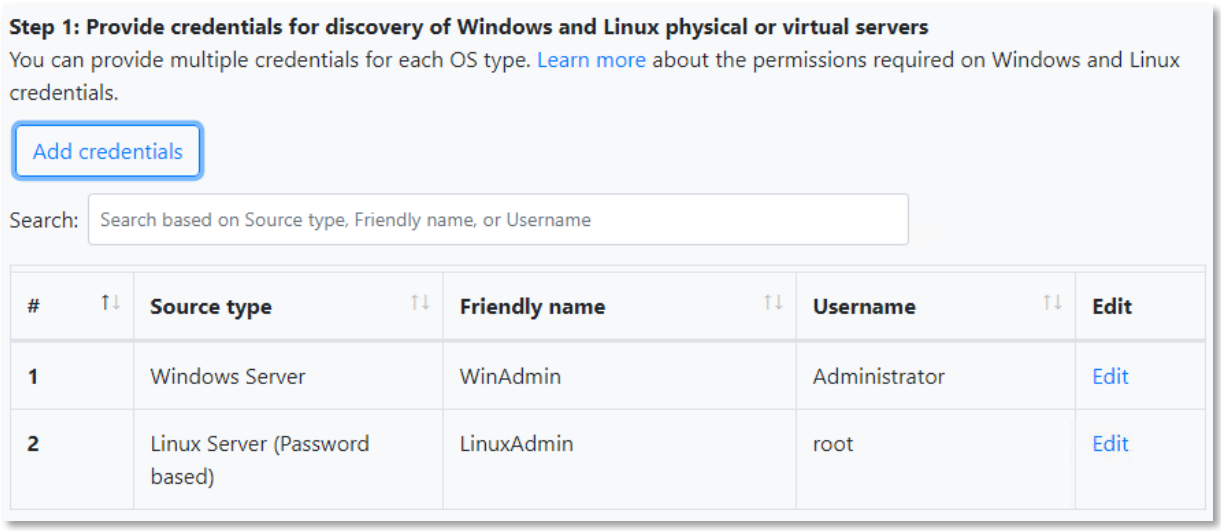
DISCOVER SERVERS FOR ASSESSMENT ON THE APPLIANCE SERVER

Permissions requirements for discovery: [Azure Migrate Permissions Requirements | Microsoft Docs]

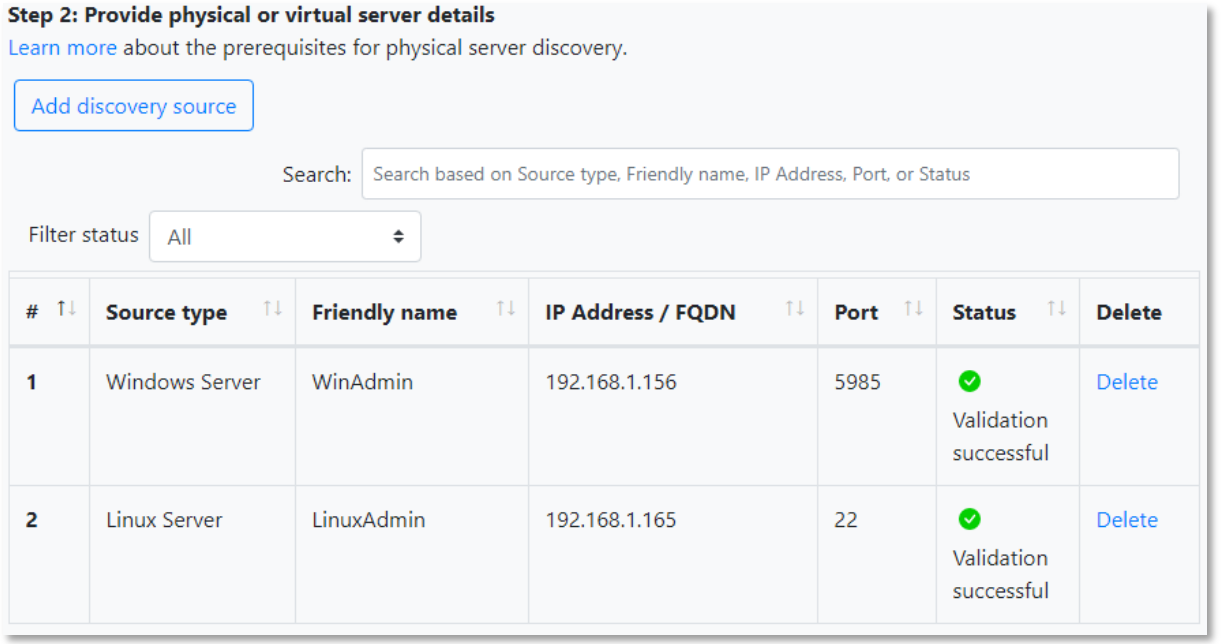
- Login to your Discovery server and open the Azure Migration Appliance Configuration Manager shortcut on the desktop.



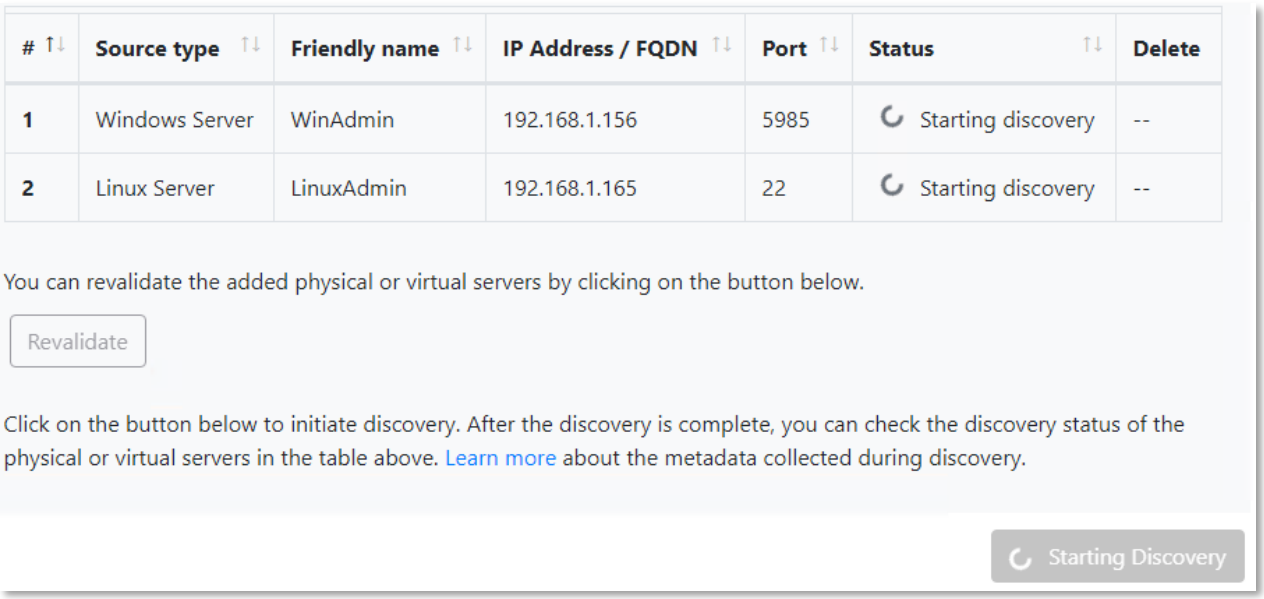
- If the system has not been accessed in some time you may need to reauthenticate with Azure.
- Add credentials for your Linux or Windows system you will be discovering for migration



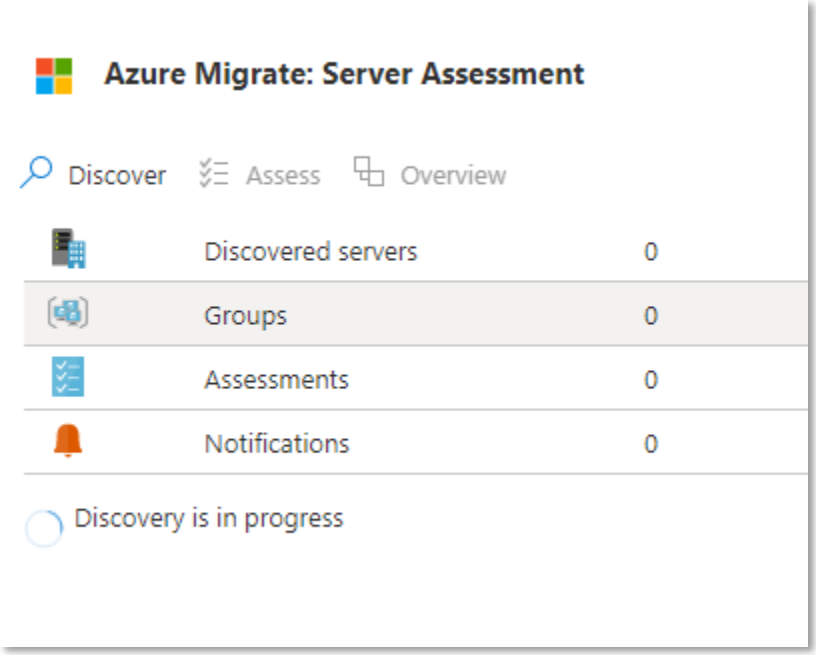
- Add your servers for discovery by entering a single item, multiple items or using a CSV file



- Once your servers have been added and validated click the Start discovery button and the discovery status will show on the status column for each server.



- Navigate to the Azure portal which will show Discovery in Progress until the process is complete.



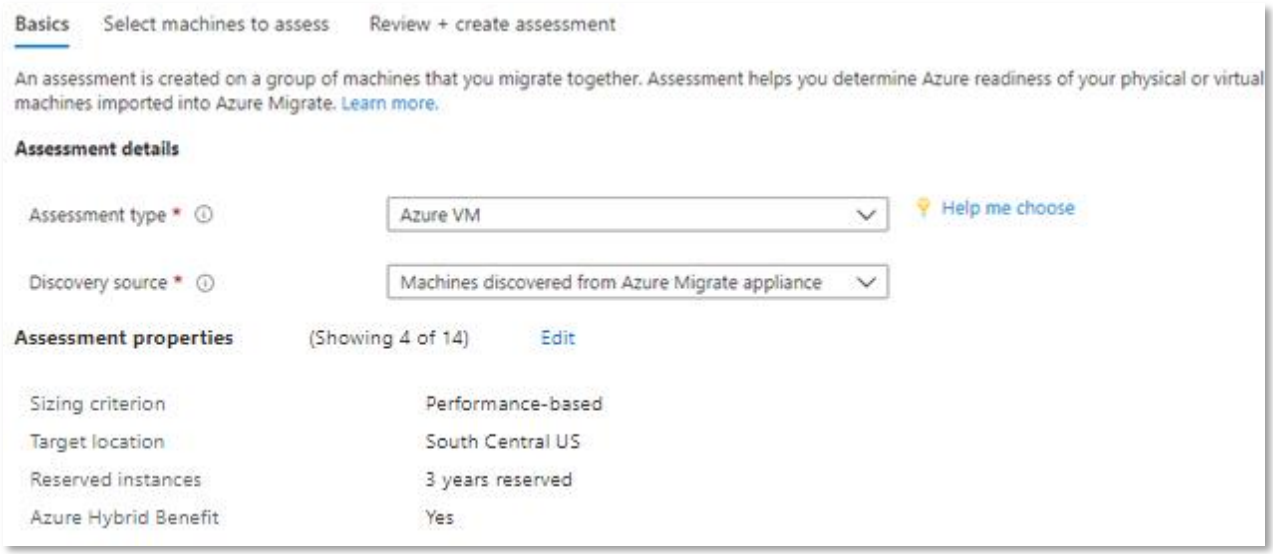
- Once the discovery is completed you can move on to performing the server assessment

RUN AZURE MIGRATE ASSESSMENTS IN THE PORTAL/REVIEWING ASSESSMENTS

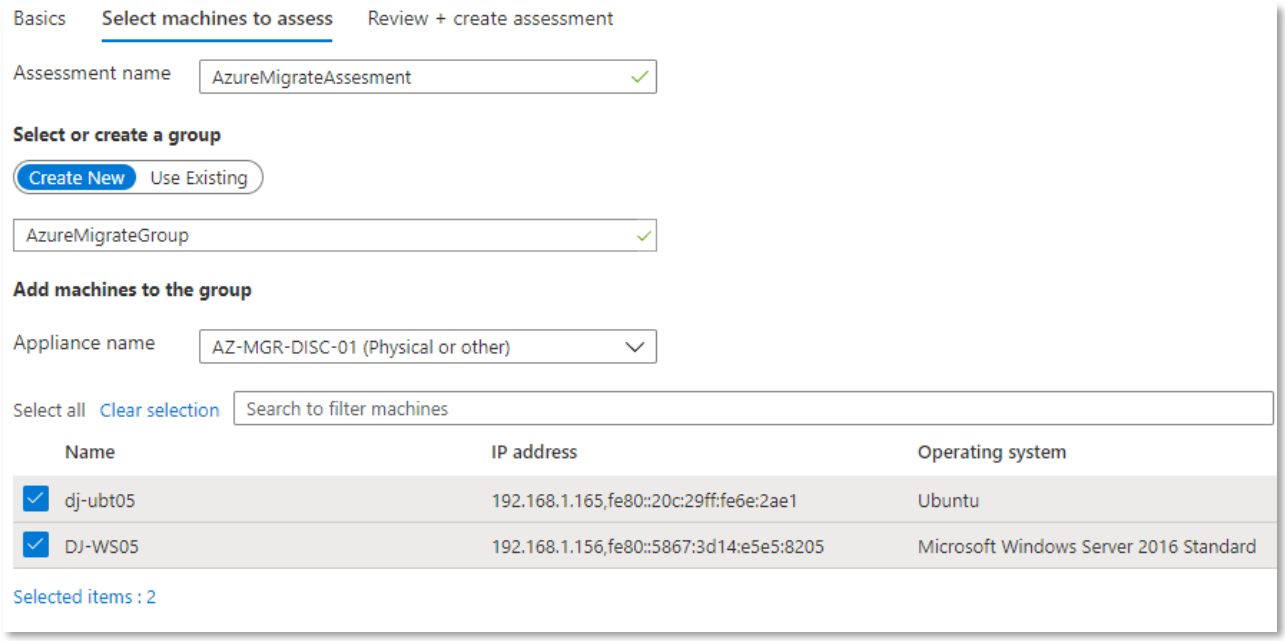
Azure Migrate assessment options: [Azure Migrate assessment types | Microsoft Docs]

Running Azure Migrate Assessments

- In the Azure Migrate portal once discovery completes click the Assess button to begin assessment



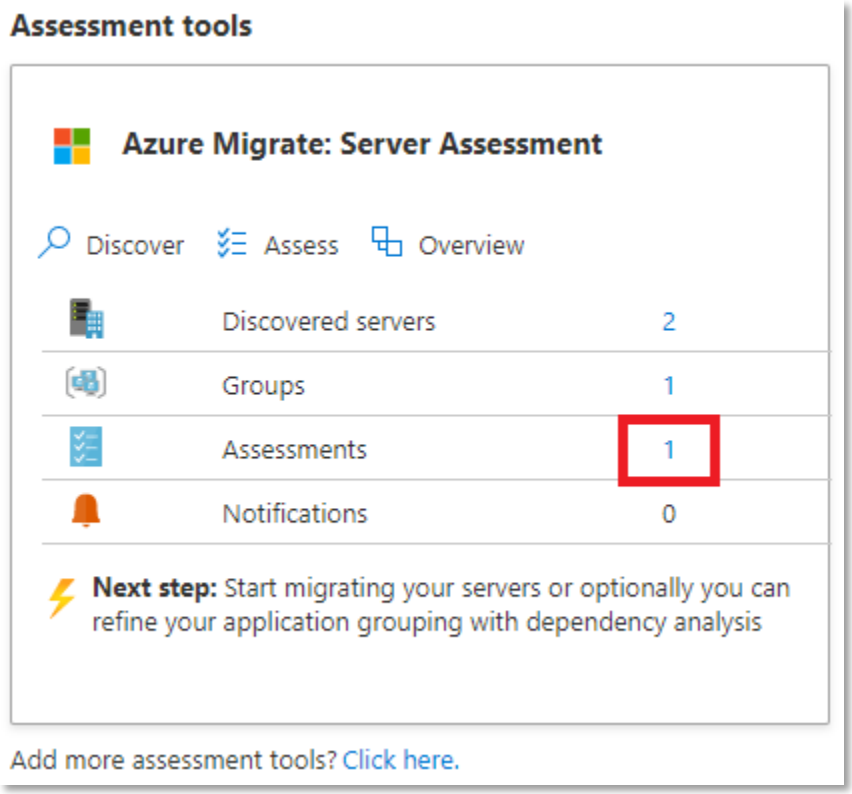
- Modify the Assessment properties to match your project needs and click Next
- Create an Assessment name, select a resource group or create one and select the servers to assess.



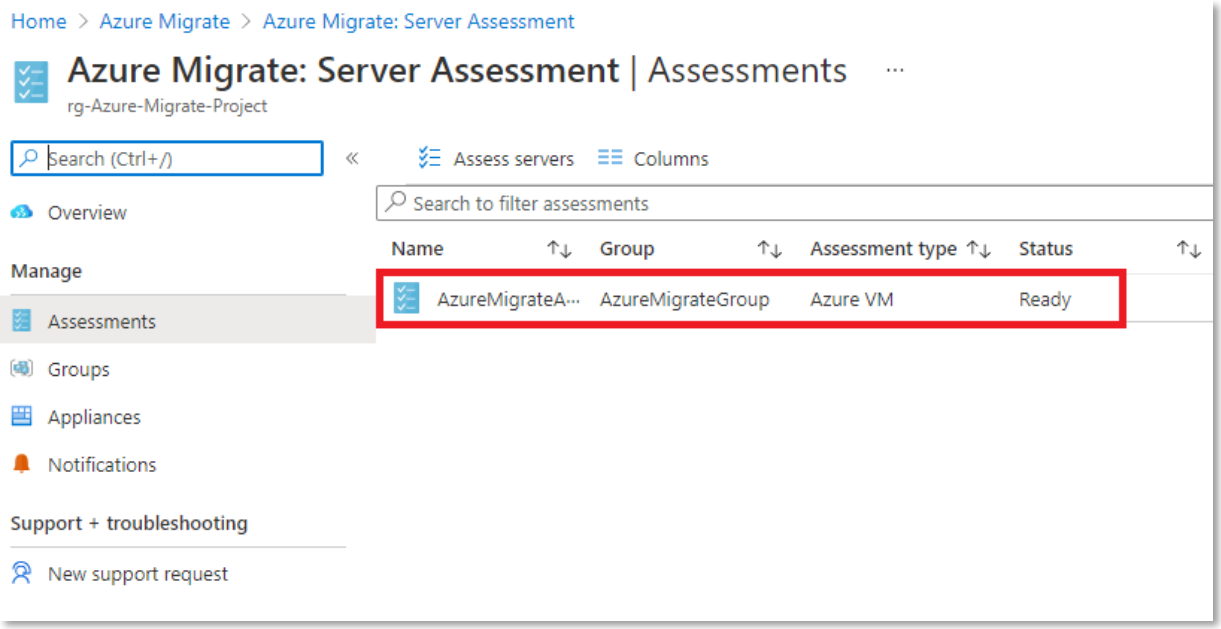
- Click Next, then Create and Assess.
- The Assessment will run and provide information within 24 hours. For the best results allow the assessment to run for a week or more for the best accuracy on system performance requirements.

Reviewing Azure Migrate Assessments

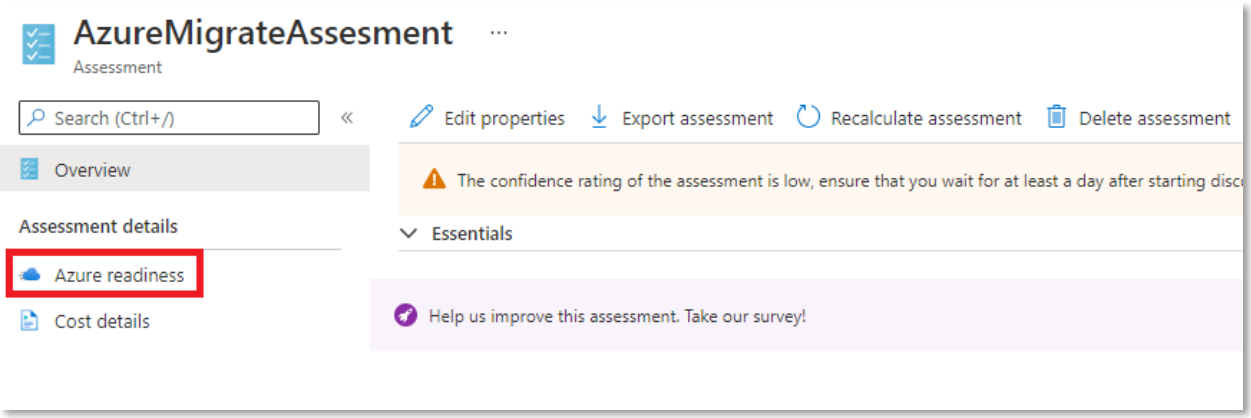
- Navigate to the Azure Migrate portal. From here we will get the server sizing settings
- Under "Assessment tools" click the blue number to the right of Assessments



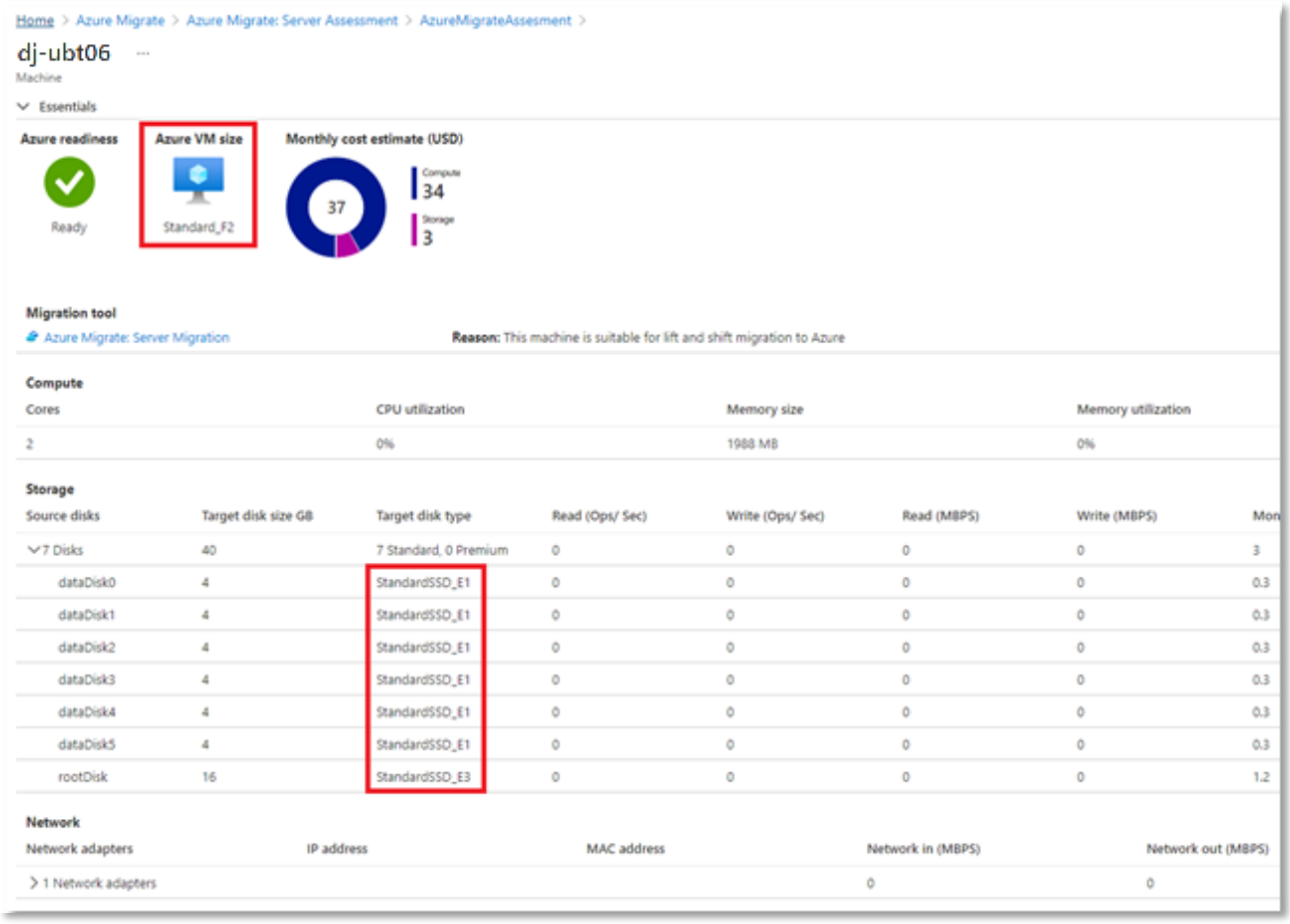
- Click into your existing assessment



- Click Azure readiness on the left hand side



- Click on the name of the server you are looking for sizing and disk information on
- From here we can get the virtual machine sizing information and disk type for the next steps in beginning replication. (In this example Standard_F2 with the disk type as Standard SSD)



INSTALL MOBILITY AGENTS ON PHYSICAL SERVERS TO BE REPLICATED

Extra Documentation: [Mobility Agent Installation Linux-Windows Azure Migrate | Microsoft Docs]

Note: In the */Platform* parameter, you specify *VMware* if you migrate VMware VMs, or physical machines.

Prerequisites

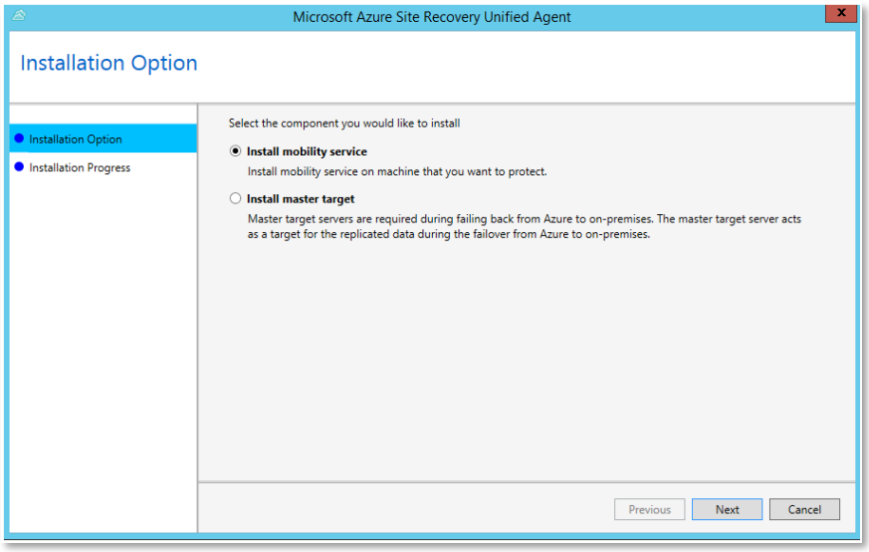
Generate Passphrase on Each Configuration Server and Locate Installer Files

- Sign in to your configuration server, and then open a command prompt window as an administrator.
- To change the directory to the bin folder, execute the following command:
    - cd %ProgramData%\ASR\home\svsystems\bin
- To generate the passphrase file, execute:
    - genpassphrase.exe -v > MobSvc.passphrase
- Your passphrase will be stored in the file located at
    - %ProgramData%\ASR\home\svsystems\bin\MobSvc.passphrase
- Locate the correct installer. Go to %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder on configuration server. Check which installer you'll need based on the following table.

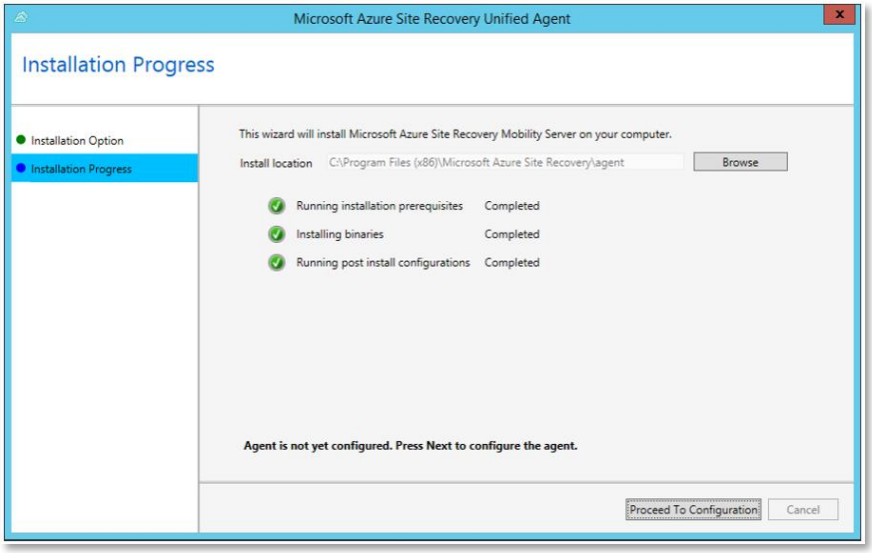
Installer file	Operating system (64-bit only)
Microsoft-ASR_UA*Windows*release.exe	Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1
Microsoft-ASR_UA*RHEL6-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 6.* CentOS 6.*
Microsoft-ASR_UA*RHEL7-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 7.* CentOS 7.*
Microsoft-ASR_UA*SLES12-64*release.tar.gz	SUSE Linux Enterprise Server 12 SP1,SP2,SP3
Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP3
Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP4
Microsoft-ASR_UA*OL6-64*release.tar.gz	Oracle Enterprise Linux 6.4, 6.5
Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz	Ubuntu Linux 14.04
Microsoft-ASR_UA*UBUNTU-16.04-64*release.tar.gz	Ubuntu Linux 16.04 LTS server
Microsoft-ASR_UA*DEBIAN7-64*release.tar.gz	Debian 7
Microsoft-ASR_UA*DEBIAN8-64*release.tar.gz	Debian 8

Windows GUI Install

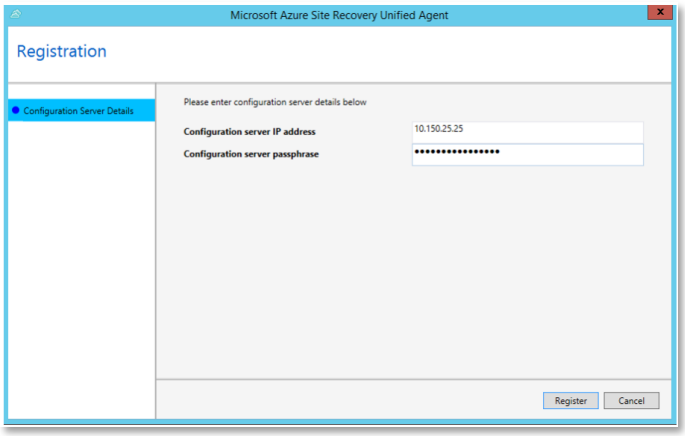
- Copy the installer and the passphrase file to a local folder (for example, c:\Temp) on the server that you want to protect and run it.
- In installation option, select install mobility service.
- Select the installation location > Install.



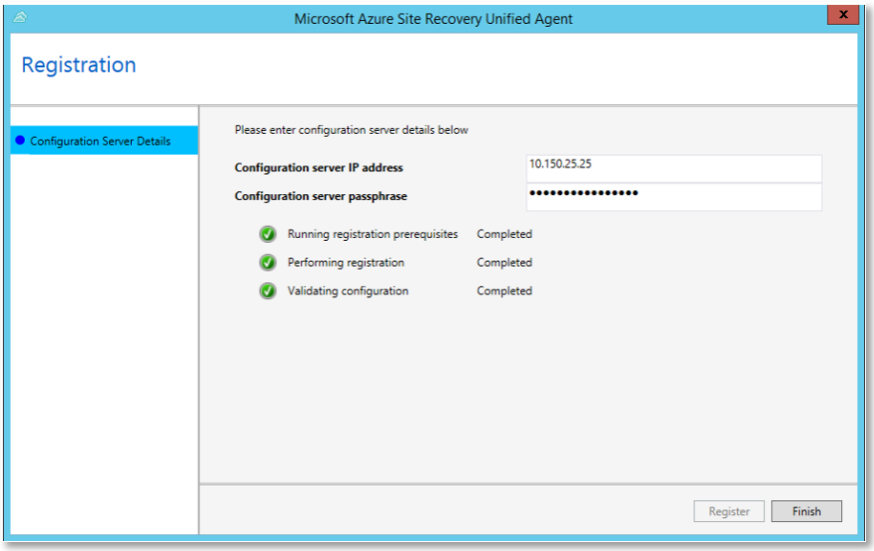
- Monitor the installation in Installation Progress. After the installation is finished, select Proceed to Configuration to register the service with the configuration server.



- In Configuration Server Details, specify the IP address and passphrase from the passphrase file you copied.



- Select Register to finish the registration.



Windows Command Line Install

- Copy the installer and the passphrase file to a local folder (for example, C:\Temp) on the server that you want to protect

- Open a command prompt as Administrator

- Extract the agent installer by running the following commands:

  ```
  cd C:\Temp
  ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe
  MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted
  cd C:\Temp\Extracted
  ```

- Run the following commands to install the Mobility Service:
  ```
  UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery" /Platform "VmWare" /Silent
  ```

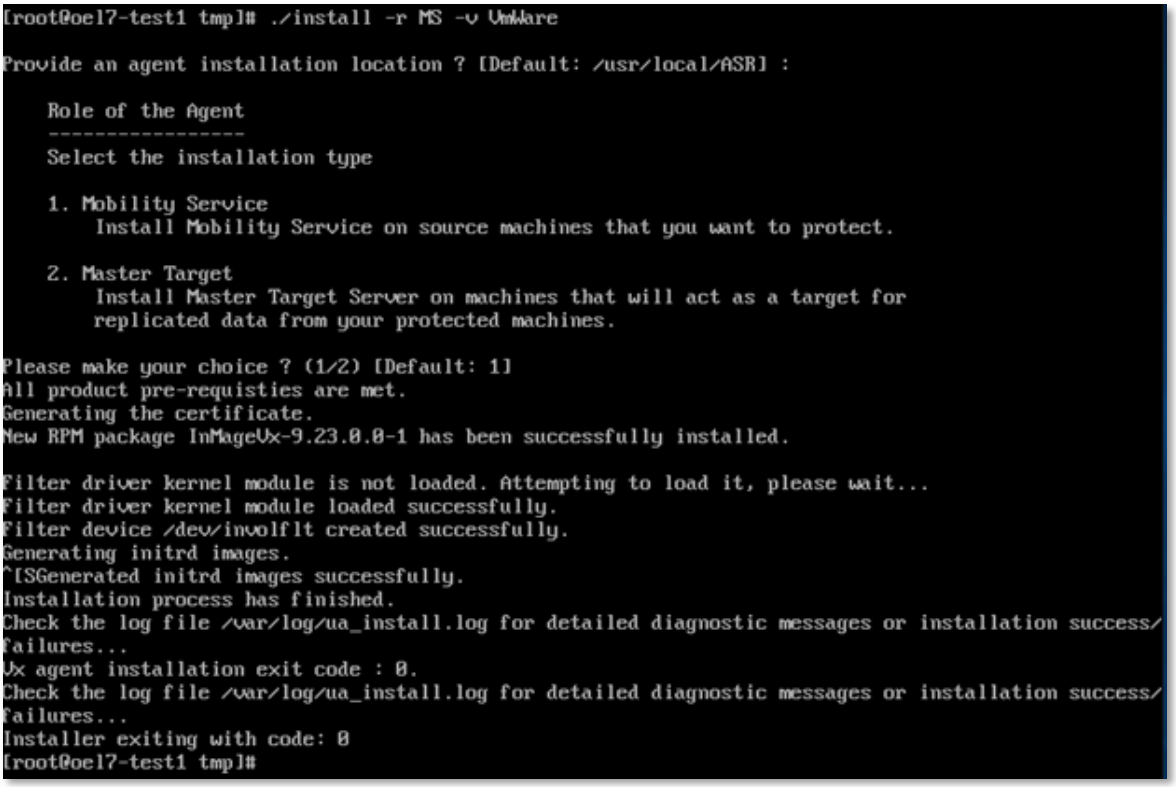
- After installation is finished, the Mobility Service must be registered to the configuration server. Run the following commands to register the agent with the Configuration Server:
  ```
  cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent
  UnifiedAgentConfigurator.exe  /CSEndPoint <IP of Configuration Server> /PassphraseFilePath <PassphraseFilePath>
  ```

Linux Install

- Copy the installer and the passphrase file to a local folder (for example, /tmp) on the server that you want to protect. In a terminal, run the following commands to change to the directory with the installer tar file and extract it:

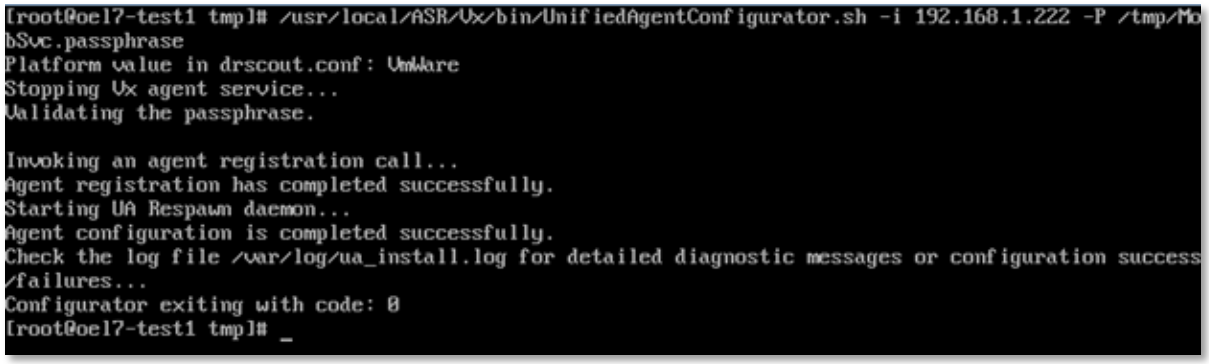
  cd /tmp
  tar -xvf <filename>

- Install with the following command:
  sudo ./install -r MS -v VmWare



- After installation is finished, the Mobility Service must be registered to the configuration server. Run the following command to register Mobility Service with the configuration server:

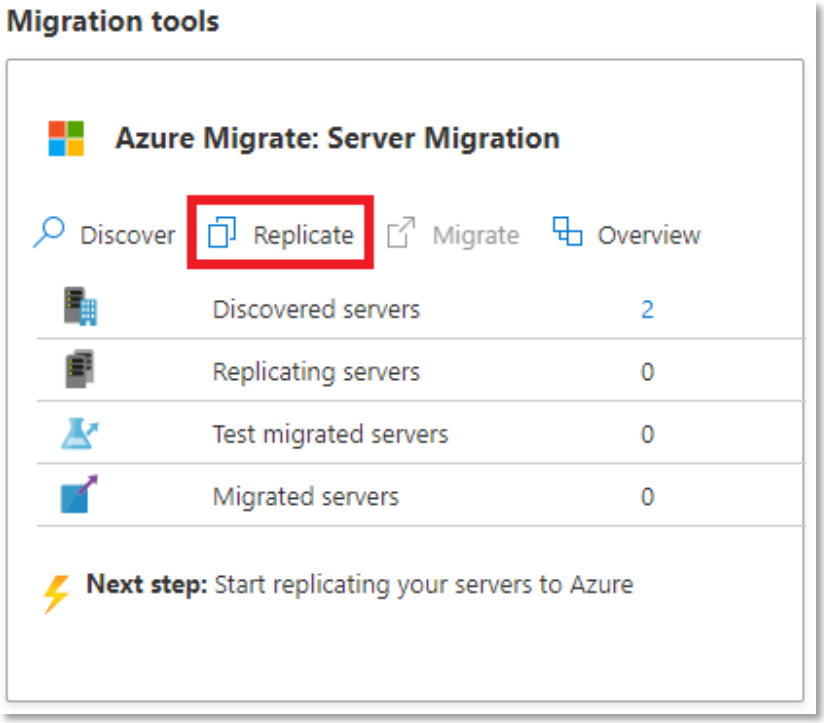
  /usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <IP of Configuration Server> -P /tmp/MobSvc.passphrase



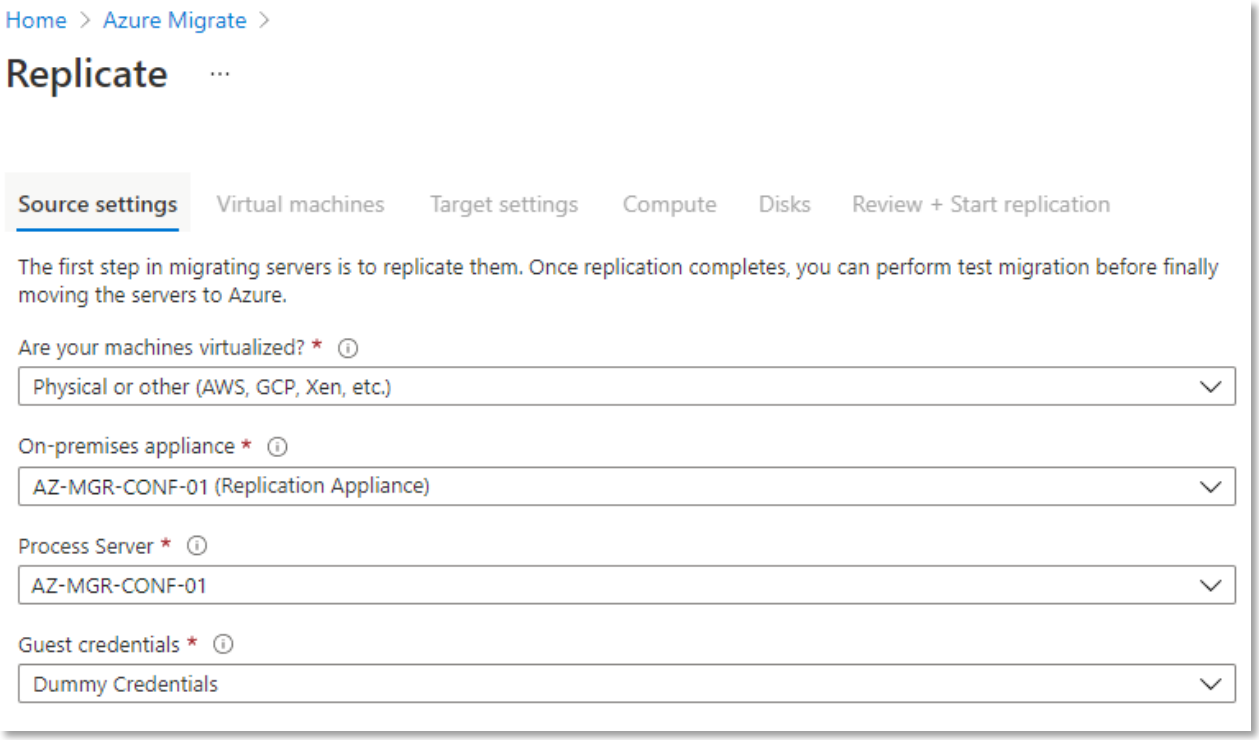
BEGIN REPLICATION THROUGH AZURE MIGRATE

Prerequisites: Mobility Agent installed and configured on any servers to be replicated

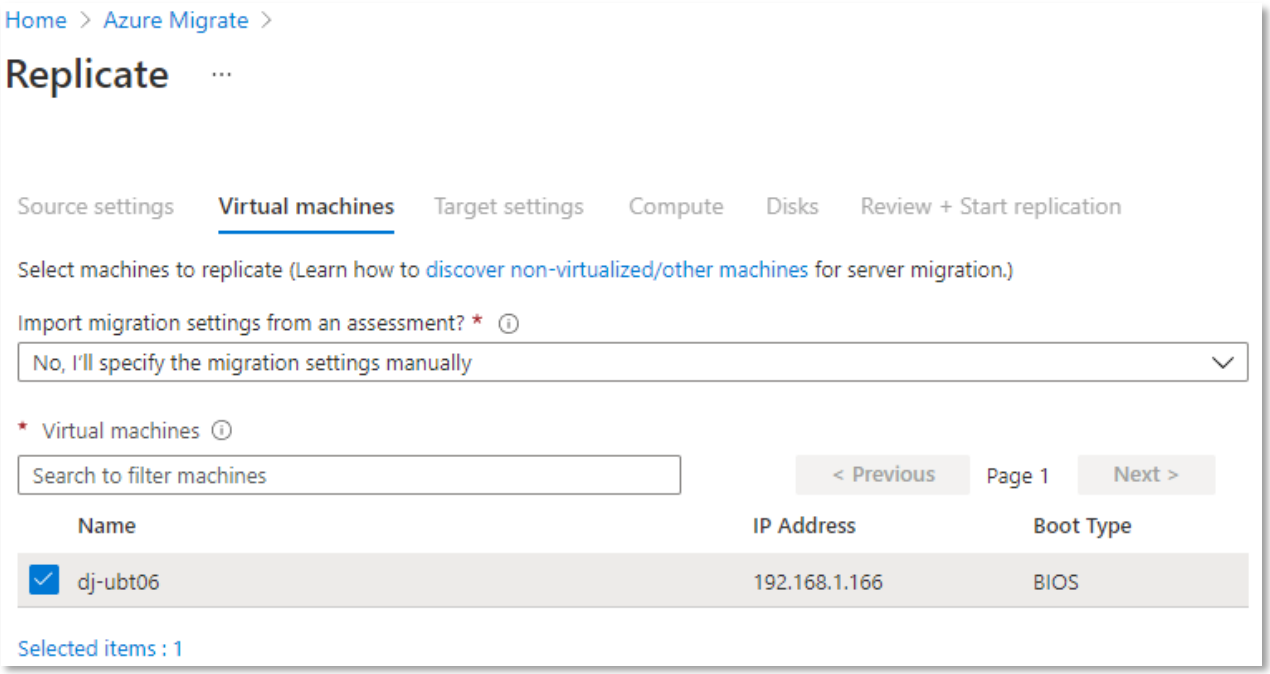
- In the Azure Migrate portal click the Replicate button under the Azure Migrate: Server Migration section



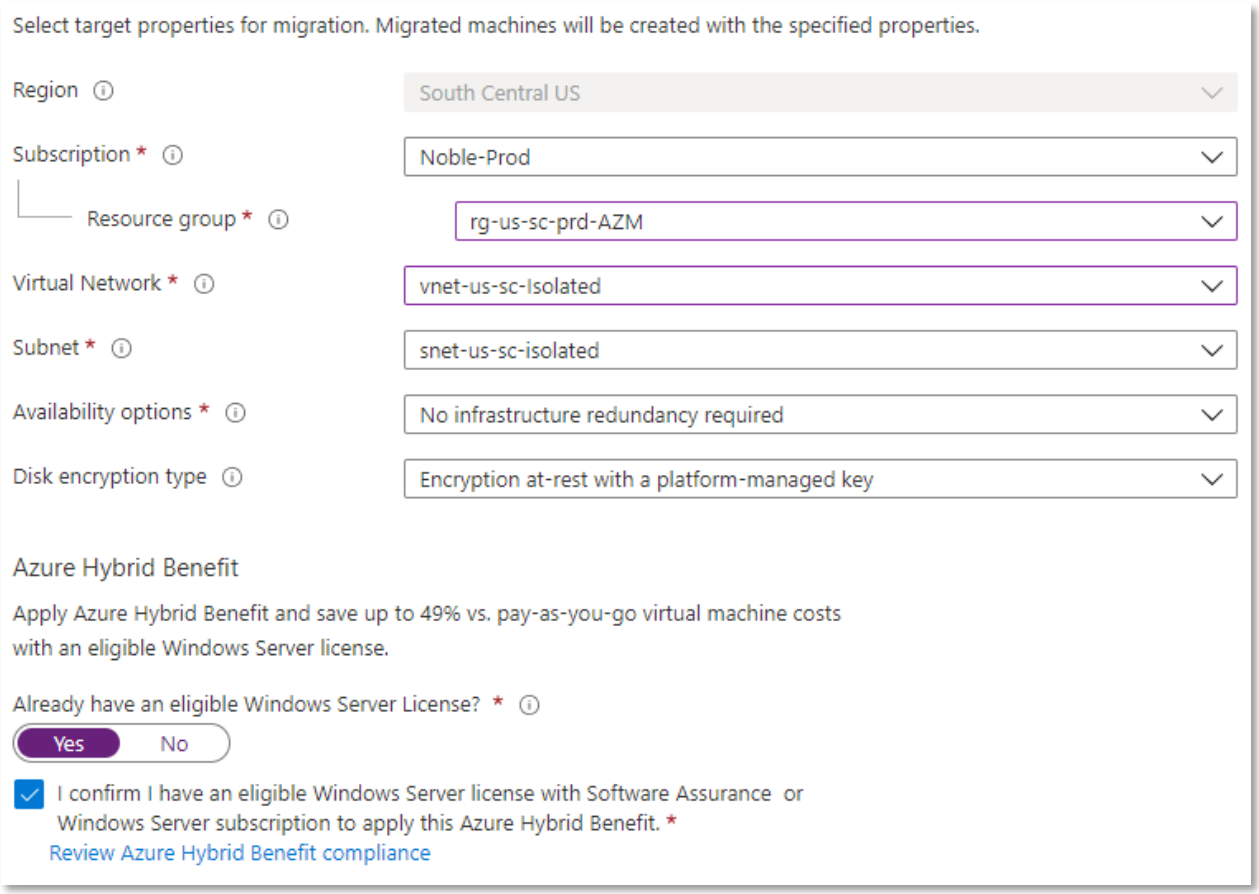
- Select Physical or other for the virtualization dropdown and verify your configuration server is selected along with the dummy credentials created with the configuration server.



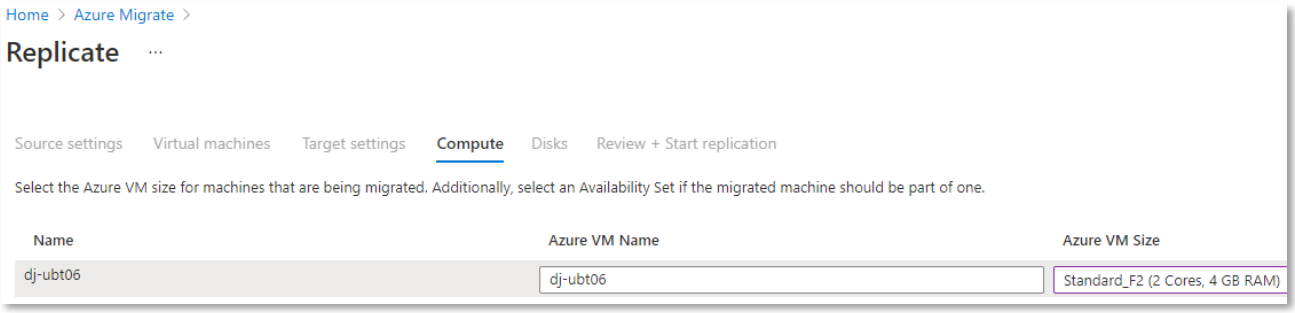
- On the next screen select "No, I'll specify the migration settings manually" and select the server(s) to migrate



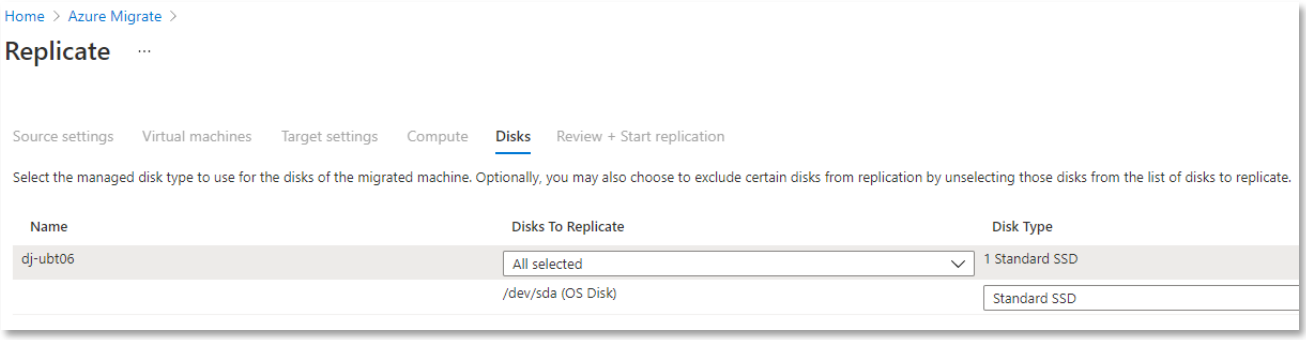
- Select the proper subscription, resource group and target vnet/subnet settings for your server
- If applicable apply the Azure Hybrid Benefit to reduce server licensing costs



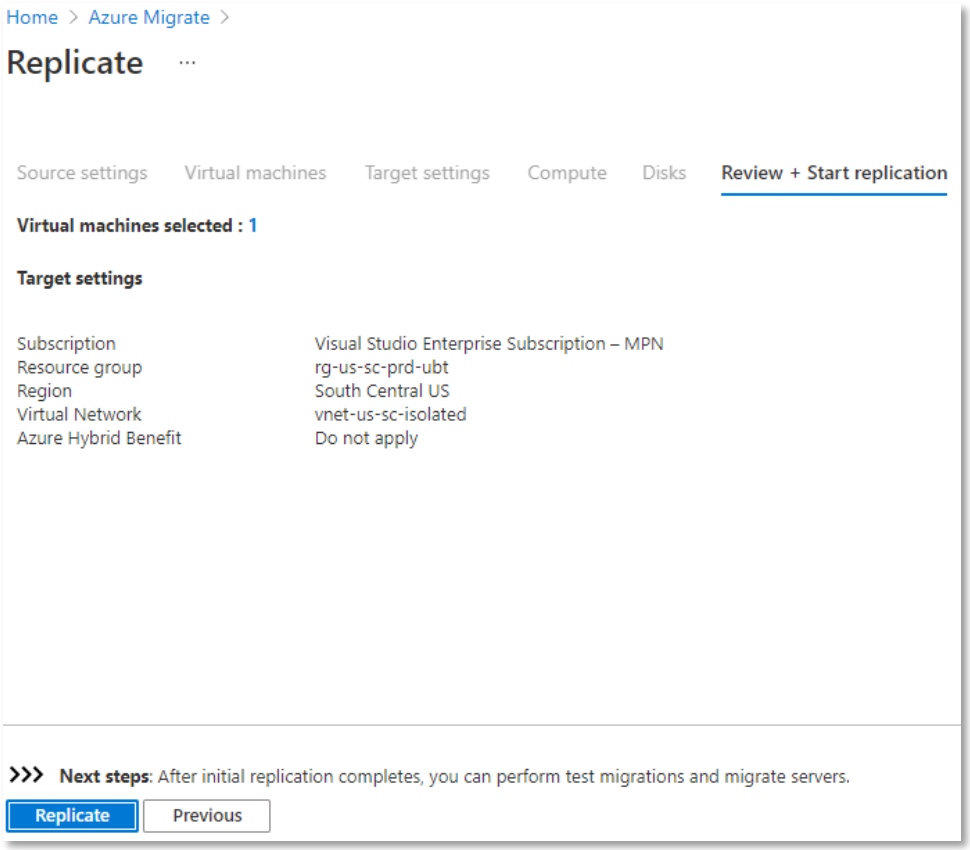
- On the next screen we will select the virtual machine sizing options (CPU and RAM configuration). Refer to the assessment created earlier for accurate right sizing.
- Switch back to your previous tab with the replication settings for compute sizing and enter the information from your Azure Migrate assessment.



- Select Next and on the Disks, screen select the disk type specified in our assessment
- The disk type you specify here cannot be changed unless replication is restarted or until after failover

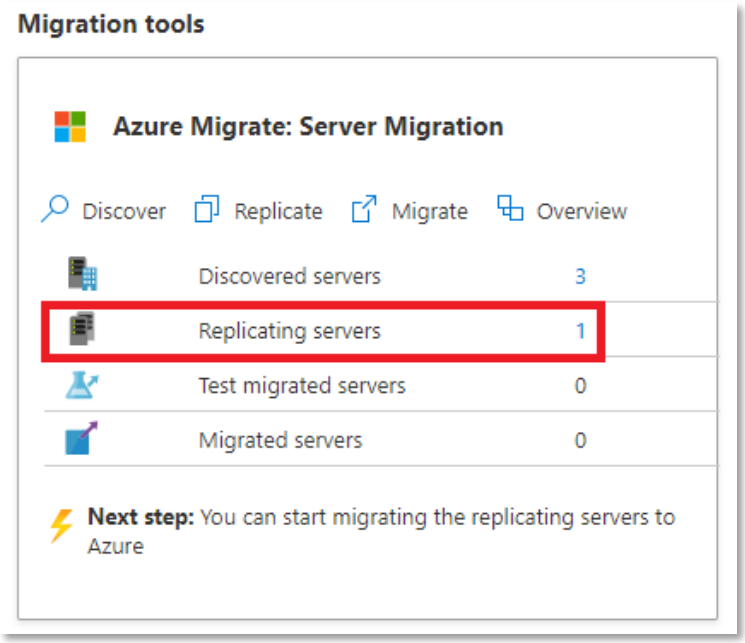


- Click next to review the configured Target settings and if everything is correct click Replicate

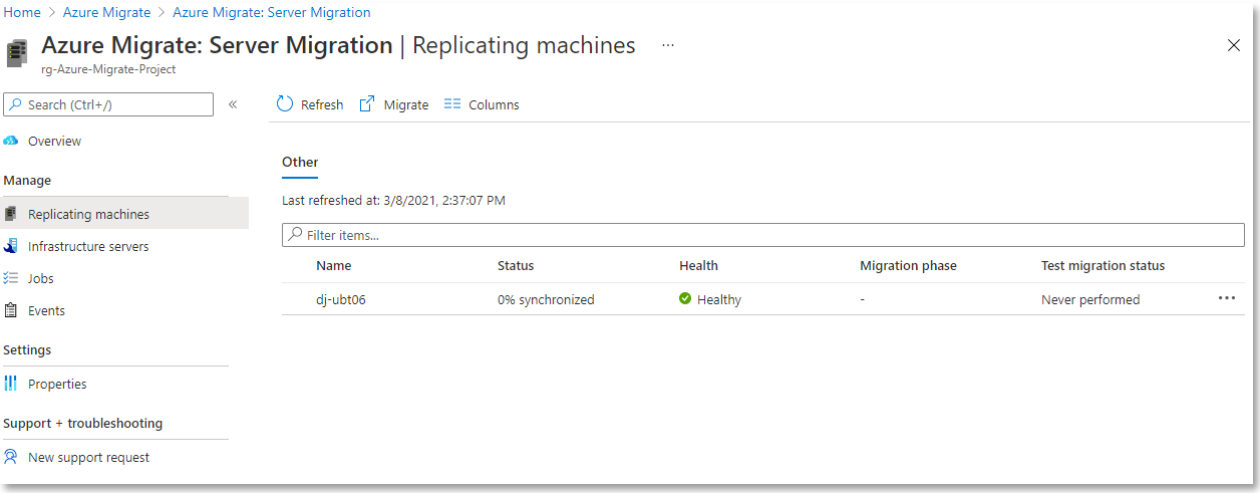


CONFIGURE MIGRATION SETTINGS OF REPLICATED SERVERS

- Once a server is replicating you may need to adjust the sizing or network settings before failover
- To do this click on "Replicating servers"

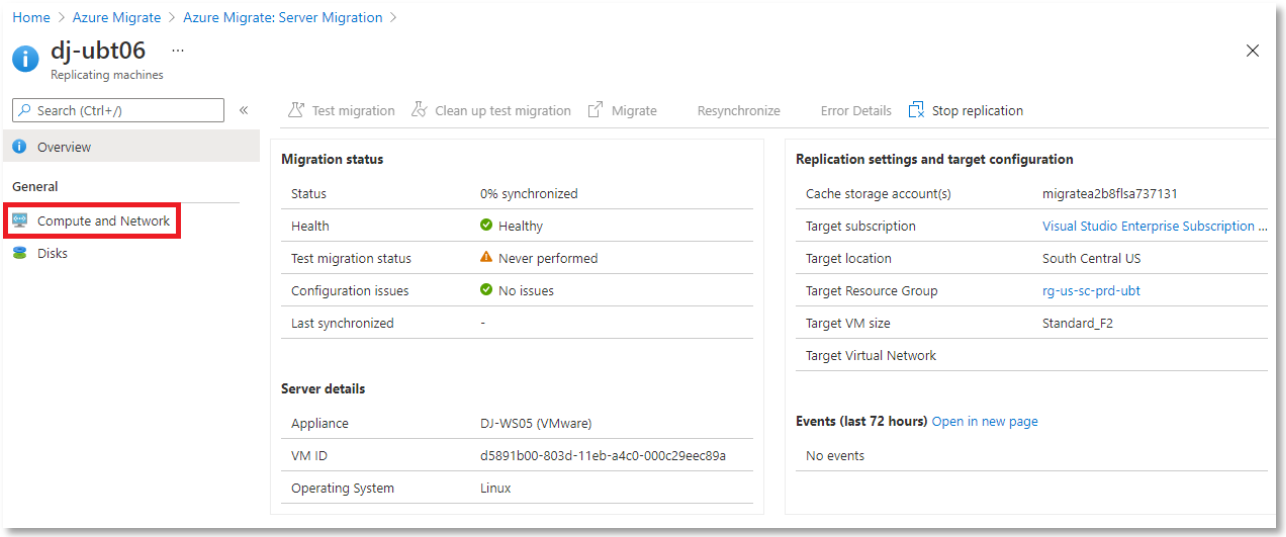


- You will be presented with a list of the replicating servers from here you can click on the server you would like to adjust sizing or network information on.

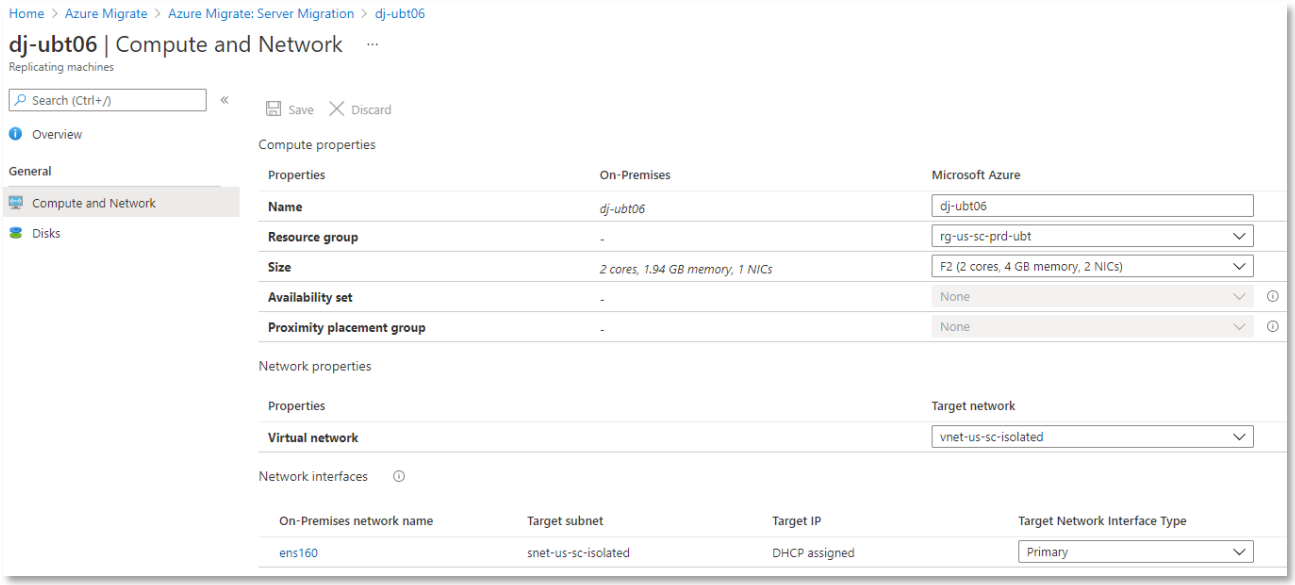


- Once you click the appropriate server you will be presented with an overview of the information available

- Clicking Compute and Network along the left side will allow you to view and adjust those settings



- Click Edit at the top of the screen to allow you to adjust any of the available settings
- Once done make sure to click Save

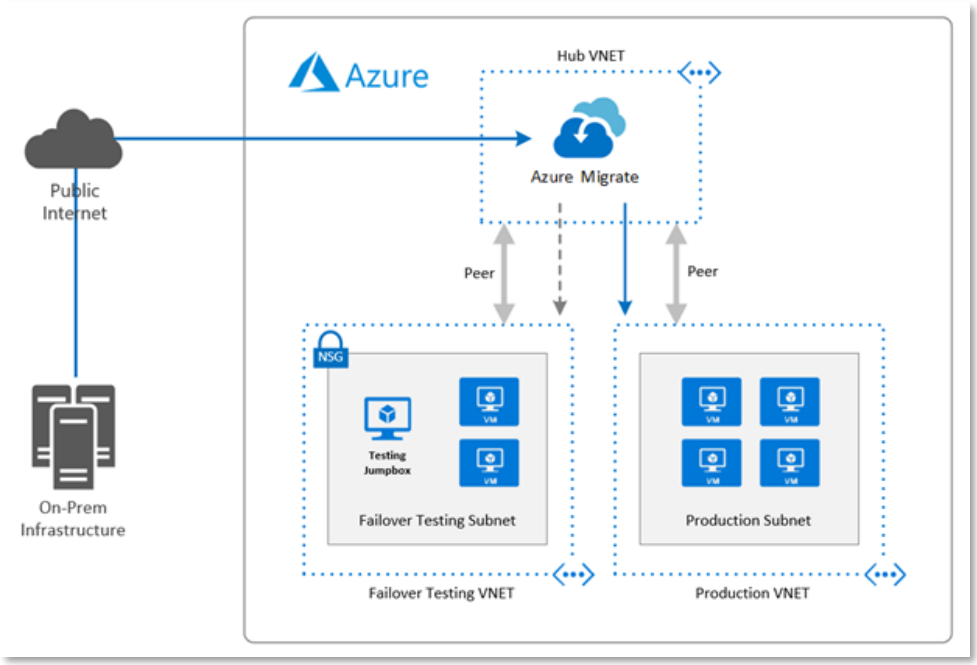


FAILOVER TESTING SETUP

Failover testing should take place before migrating into a live production Azure environment. During failover testing, VMs are brought online from the replicated server or workload data that has been copied to Azure storage. The VMs are created and brought online in an isolated or semi-isolated environment while the production on-premises source VMs are left online. Since the on-premises machines are online during this testing, It is important that the landing network is isolated to prevent Active Directory trust conflicts, testing server registration into production DNS, unwanted communication to production resources, etc.

A typical isolated testing environment would consist of a VNET that is peered to your hub network, a failover testing VNET and subnet, an NSG that isolates all but necessary traffic (such as RDP), and a jump box if desired.

Typical Failover Testing Topology



Failover Testing Procedure

Failover testing should be a collaborative effort between the migration team and the workload/application team. After the source workloads have been replicated and are in sync to the desired RPO, A test failover via Azure Migrate will be initiated.

Infrastructure and application teams should participate and test as much as possible. If application testing is possible, it is highly recommended.

Failover Testing Checklist

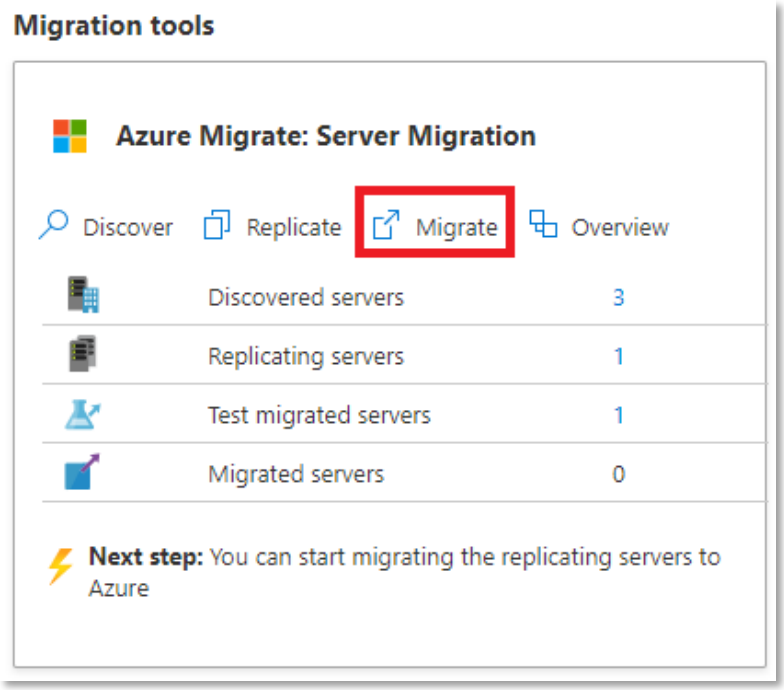
- ☐ Does the server boot as expected to the login screen? This can be checked via boot diagnostics?
- ☐ Did the server boot normally within the typical boot time without any new errors?
- ☐ Is the server accessible over the network?
- ☐ Is there any new latency experienced that is not acceptable?
- ☐ Can you log into the server as expected? During failover testing it may only be possible to test local logins due to the NSG blocking communication to an Active Directory.
- ☐ Are any new errors being reported in the system or application logs that may indicate a problem?
- ☐ Are disks mounted, appear to be at RPO, and in a healthy state?
- ☐ If possible, test disk performance to ensure deployed level of performance is acceptable.

- ☐ Are any services in a failed state that should be running? Will they start normally?
- ☐ If any services failed on first boot, do they start normally on following reboots?
- ☐ Are any new errors being reported in the system or application logs that may indicate a problem?
- ☐ If possible, test server or application performance against a benchmark. Should resizing be considered?

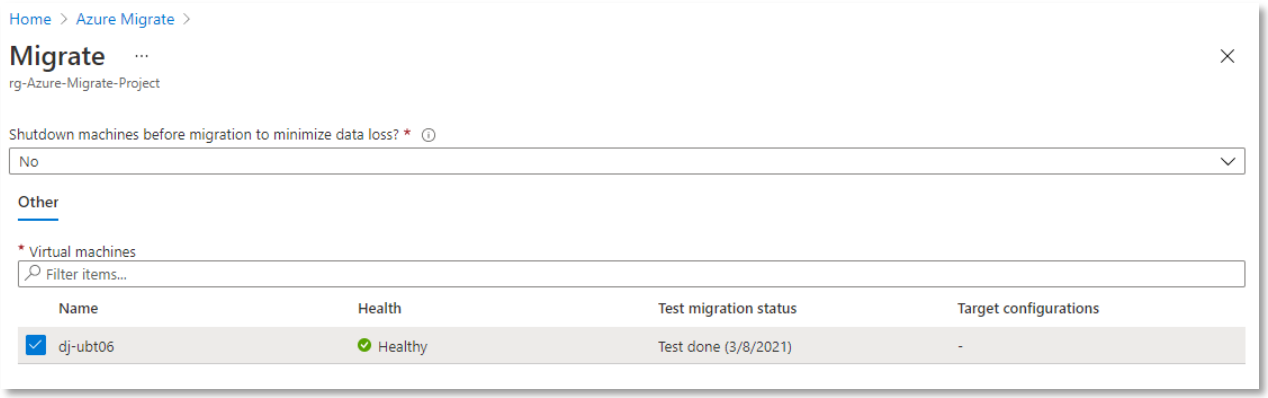
MIGRATION IN AZURE MIGRATE

Once your server(s) are fully replicated to Azure and a test failover has been performed you can begin migration planning. A time should be chosen to minimize impact to the workload/application you are migrating. Make sure all applicable/infrastructure teams are involved and available.

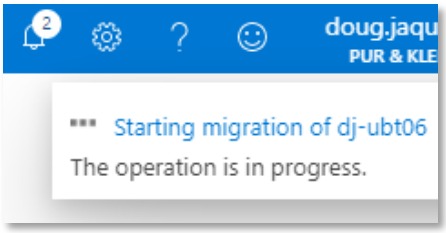
- To begin the migration navigate to the Azure Migrate portal
- Click Migrate under the Migration tools section



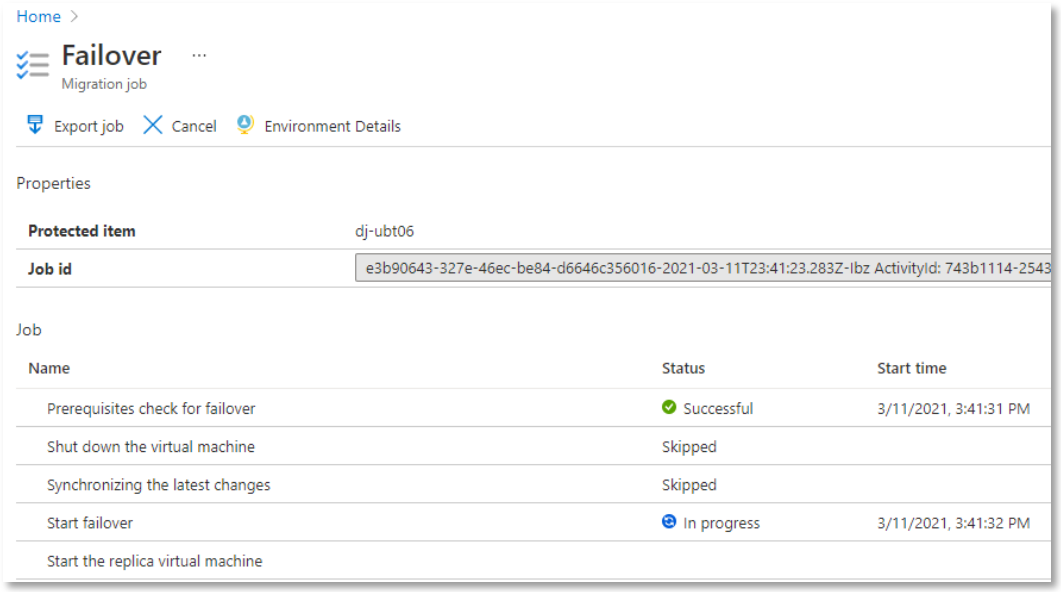
- Select the server(s) you wish to migrate, on the next screen and select Migrate
    - Select No for "Shutdown Machines before migration" as ***with Physical migrations Azure migrate will not shutdown the server if you select Yes. Make sure to shutdown the server manually once you start the migration process.***



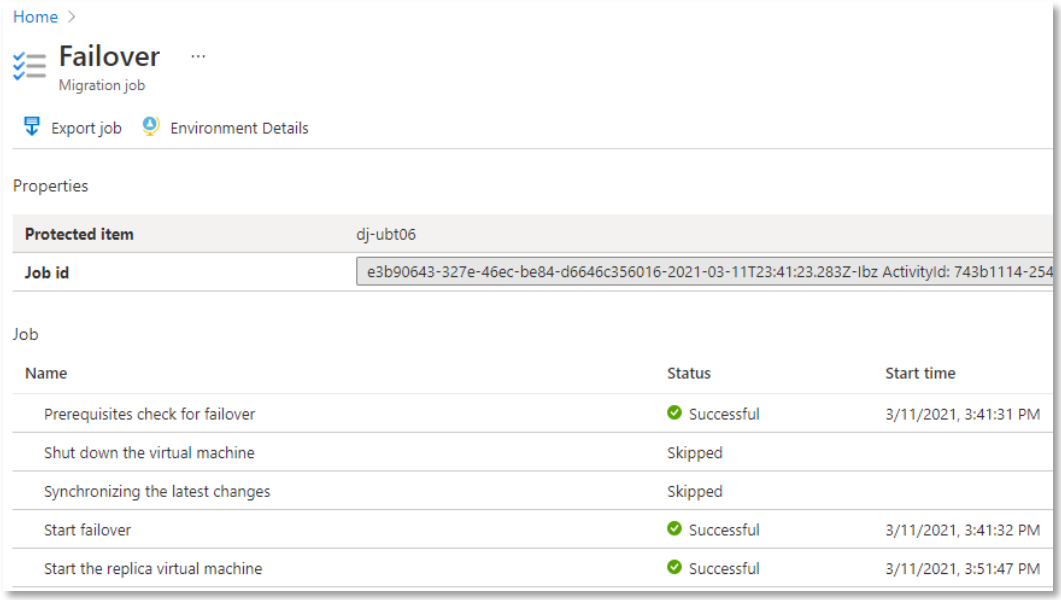
- Click the bell icon at the top right and then the migration event to see each step of the migration process



- Here you can see a migration in process



- Once the migration is complete you will see the following screen, you may now begin testing



MIGRATION/APPLICATION/SERVER TESTING

Application testing should be performed after failover and infrastructure testing has passed validation. Application testing should be performed by the team that is responsible for the workload or applications that are being migrated. Since this workload is now considered production, we recommend that you perform any QA, benchmark, or load testing that would normally be performed after maintenance to ensure the application is performing as expected in Azure.

Application Testing Procedure

The application testing procedure should be defined by the application team. This procedure should be a based on any QA, benchmark, or load testing used in standard QA testing, maintenance, or upgrade testing. We suggest that you develop and have this process well documented, planned, and staffed before the migration.

Application Testing Checklist

Since application testing is performed by the application team that understands the workload, we can only provide a very basic checklist. We suggest that you develop and have this process well documented before the migration.

- ☐ Did the applications start as expected?
- ☐ If applications did not start as expected, do they start after a reboot of the workload servers in the correct order?
- ☐ Are databases used by the workload accessible and performing as expected?
- ☐ Is there any new network latency introduced after the migration that is affecting performance of the application or parts of the application? Is it acceptable?
- ☐ Is the workload accessible from the expected URL or endpoint?
- ☐ Are end users able to access and login to the application and interact with it as they normally would?
- ☐ Are the application performance meeting predefined benchmarks and/or end user expectations?
- ☐ Are any new errors being reported in the system or application logs that may indicate a new problem?
- ☐ If possible, test disk performance to ensure deployed level of performance is acceptable.
- ☐ Test application performance against a benchmark. Should resizing of any virtual machines be considered?

POST FAILOVER CONFIGURATIONS

Following a failover, steps should be taken to configure operations on the migrated VMs to ready them for production. When the VMs have been tested and the migration has been declared a success, the replicated items need to be cleaned up so they are removed from the Recovery Services Vault.

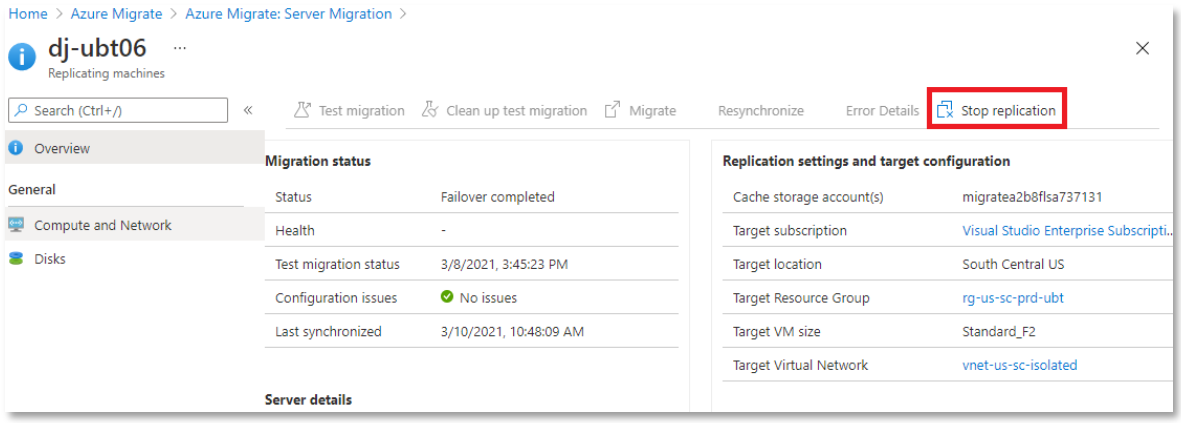
Recommended post failover configuration

- Connect the VMs to a Log Analytics Workspace
- Enable Azure backups
- Apply Tags to migrated resources
- Verify boot diagnostics are configured and using a shared storage account
- Enable extended diagnostics if desired
- Add to a patching schedule
- Verify monitoring, change tracking, enable EMS, or any other desired platform features
- Optimize the OS for Azure – move the pagefile to the Azure temp disk, reconfigure boot settings, etc. Guidance can be found here - [Microsoft Docs | Prepare VM's for migration]

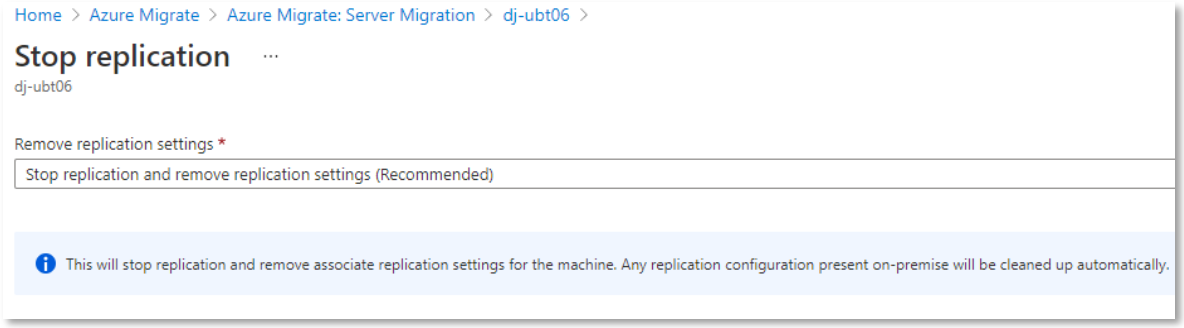
Note: The Azure VM agent is not supported on 32-bit operating systems. Certain platform features such as backups, VM extensions, run command, and any other features requiring the Azure VM agent will not be available.

Post Failover Cleanup

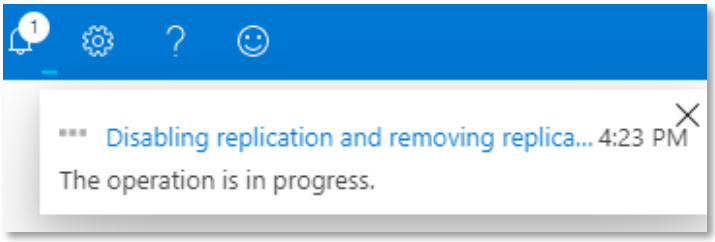
- Once the migration is successfully finished post migration cleanup can be performed. This includes stopping the replication to complete the migration. Navigate to the VM in the Azure Migrate project. Then select Stop replication.



- Select "Stop replication and remove replication settings" in the dropdown and click OK.



- The removal process will begin and notify you of any errors via the activity log



- We recommended that following a migration, whether successful or not, that a meeting is facilitated between all teams involved to discuss successes and misses during the migration. This will allow for continual improvements in the migrations process and execution, as well as help document known or newly discovered issues and prevent future problems.

INFRASTRUCTURE TESTING

Infrastructure testing should take place after failover testing has been completed and any problems or concerns that were discovered have been resolved. During failover, Azure VMs are brought online from the replicated server or workload data that has been copied to Azure storage. The VMs are created and brought online in the production Azure environment and the production on-premises source VMs are shut down.

After failover, the Azure machines should be considered as production, and tested accordingly. It is critical that infrastructure and application testing are thorough to ensure that any problems are discovered and are resolved as quickly as possible.

Infrastructure Testing Procedure

Infrastructure testing should be a collaborative effort between MBG and the client team. After the source workloads have been replicated and are in sync to the desired RPO and failover testing is complete, MBG will initiate the failover via Azure Site Recovery or Azure Migrate during the designated window and provide basic testing, as level of granted access allows.

Client infrastructure teams should participate and test as much as possible.

Infrastructure Testing Checklist

- ☐ Does the server boot as expected to the login screen? This can be checked via boot diagnostics?
- ☐ Did the server boot normally within the typical boot time without any new errors?
- ☐ Is the server accessible over the network?
- ☐ Are DNS lookups resolving the new Azure IP as expected?
- ☐ Is there any new latency experienced that is not acceptable?
- ☐ Can you log into the server as expected?
- ☐ Are any new errors being reported in the system or application logs that may indicate a problem?
- ☐ Are disks mounted, appear to be at RPO, and in a healthy state?
- ☐ If possible, test disk performance to ensure deployed level of performance is acceptable.
- ☐ Are any services in a failed state that should be running? Will they start normally?
- ☐ If any services failed on first boot, do they start normally on following reboots?
- ☐ Are any new errors being reported in the system or application logs that may indicate a problem?
- ☐ Test server performance against a benchmark. Should resizing be considered?

ROLLBACK

At times, unforeseen problems arise that may require a migration to be rolled back. Using Azure Migrate makes this process simple and it can be performed quickly to minimize downtime.

Rollback Procedure

During testing, if a problem is discovered that cannot be resolved, or cannot be resolved in the designated failover window, the migration or the workload, or parts of the workload will be marked as failed and a rollback will be initiated. This will be a collaborative effort that will involve both Azure and on-prem resources and will require team resources with access to perform the activities. It is the responsibility of the testers to call out any failures in a timely fashion so they can be discussed, and a go / no-go decision can be made by the proper party.

	Action items
☐	Stop the VMs targeted for rollback in Azure.
☐	Remove protected items from replicated items in Azure Migrate project.
☐	Start the source VMs on-premises.
☐	Reverse any DNS changes made during the migration.
☐	Verify login to the VM and that Active Directory trust has not been broken (Windows)
☐	Perform infrastructure testing on the on-premise VMs to verify they are back up and functioning as expected.
☐	Verify end users can access the servers and applications that have been rolled back and interact with them normally.
☐	Disable and restart replication of the VMs in Azure Migrate to re-establish sync.
☐	Gather all details of the problem that forced the rollback and schedule a planning session to determine remediation steps and how to proceed.