Migrationplan

First phase is prepare, you need to make sure that you have an on-prem machine that has Windows 2016 or newer installed with minimum of 16GB RAM, 8vCPU, and approximately 80GB disk space and preferable a secure connection to Azure example a proxy or VPN.
An inbound connection on WinRM port 5985 to ensure that Azure migration Agent and Azure can get the configuration, performance and metadata. For Linux allow the inbound connection on port 22.

In Azure you have created the subscription and management groups and assigned the roles in the Access control (IAM) and Azure AD. Make sure you have **Contributor** or **Owner** role.

When preparing the physical servers, for Linux you need a root account and use the commands bellow;

setcap CAP_DAC_READ_SEARCH+eip /usr/sbin/fdisk setcap CAP_DAC_READ_SEARCH+eip /sbin/fdisk *(if /usr/sbin/fdisk is not present)*	To collect disk configuration data
setcap "cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_setuid, cap_setpcap,cap_net_bind_service,cap_net_admin,cap_sys_chroot,cap_sys_admin, cap_sys_resource,cap_audit_control,cap_setfcap=+eip" /sbin/lvm	To collect disk performance data
setcap CAP_DAC_READ_SEARCH+eip /usr/sbin/dmidecode	To collect BIOS serial number
chmod a+r /sys/class/dmi/id/product_uuid	To collect BIOS GUID

In Azure you need to set up an Azure Migrate project. After the preparing of the servers and the project created, the Azure Migrate appliance performs a server discovery and collect the data (metadata, performance, configuration etc.)

Then generate an Azure Migrate key download the Azure Migrate installer script and execute the script with the root privileges.

The installer script then install agents web application for the physical server discovery and assessments. Update a registry key and create two files “Config” and “Logs” on the following path;
%Programdata%\Microsoft Azure\Config
%Programdata%\Microsoft Azure\Logs

When that is done configure the appliances by using a machine that can connect to the appliances and go to ***https://appliance name or IP address: 44368***
Now you can check connectivity, check time sync, install updates etc.

Now we can register the appliances with Azure Migrate, paste the project key into the field and login with your azure account.

Now we will connect **from** the appliances to the physical servers.
After you have connected we can start the discovery, if you have linux servers select source type as **Linux server (Password-based, if using SSH key use SSH key-based)** !remember Azure Migrate does not support passphrase based SSH-keys!

Next for server details add discovery source and specify server IP-Adress or FQDN number and the name to connect to the server.

When clicking save the appliances will validate the connection to the servers.
(if validation fails review the status)

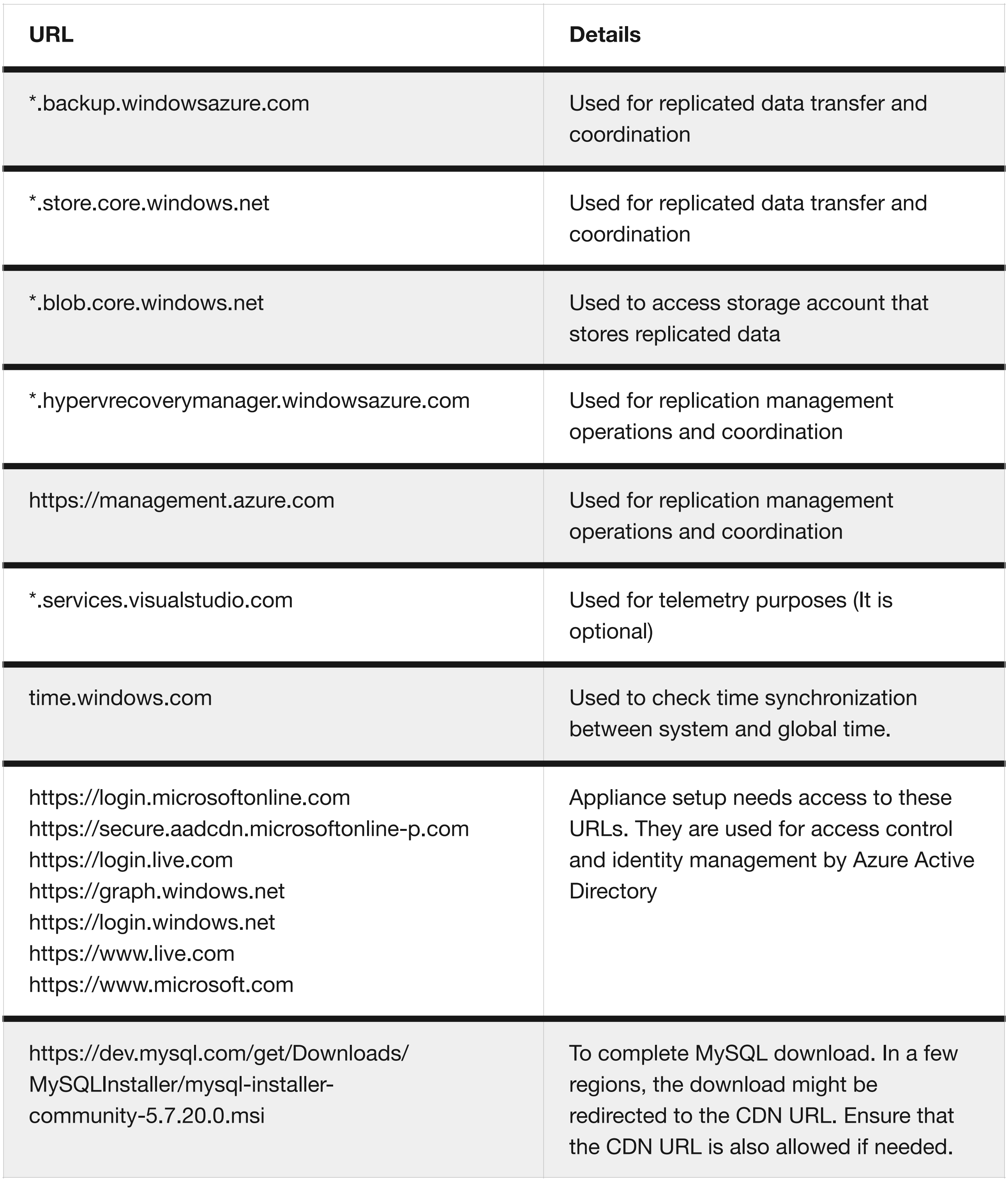
After validation the discovery is ready and will take approximately 2 minutes per server to discover metadata and for the server to appear on Azure.

After Azure have discovered the servers and they are visible in Azure we can start to assess the servers.
You can assess in two ways **As-is On-Premises** or **Performance-based** for this client we will use as-is on-premises to get the most like for like servers.

Use the Azure Migrate: Server Assessment, assessment type use **Azure VM**, in discovery source select **Machines discovered from Azure Migrate appliances** in target location use **West Europe** then select the storage type, VM size, IOPS.

When everything is provided and assessment is done it can be viewed.
An assessment is important because it describes Readiness if the servers are suitable for migration to azure, and it provides monthly cost estimation.

Now we are ready for the actual migration using Azure Migrate: Server Migration tool. We have created a project, we have assessed and we have created and viewed the permissions and requirements.
Make sure you have set up a virtual network when you migrate you need to specify a network the servers will use.
Azure Migration: Server Migration uses a replication appliance that runs the following components a **Configuration server** and a **Process server** and the appliances use a MySQL. When you go through the migration you are prompted to download and install the MySQL make sure that following URL's is accesable for the appliances;



URL	Details
*.backup.windowsazure.com	Used for replicated data transfer and coordination
*.store.core.windows.net	Used for replicated data transfer and coordination
*.blob.core.windows.net	Used to access storage account that stores replicated data
*.hypervrecoverymanager.windowsazure.com	Used for replication management operations and coordination
https://management.azure.com	Used for replication management operations and coordination
*.services.visualstudio.com	Used for telemetry purposes (It is optional)
time.windows.com	Used to check time synchronization between system and global time.
https://login.microsoftonline.com https://secure.aadcdn.microsoftonline-p.com https://login.live.com https://graph.windows.net https://login.windows.net https://www.live.com https://www.microsoft.com	Appliance setup needs access to these URLs. They are used for access control and identity management by Azure Active Directory
https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi	To complete MySQL download. In a few regions, the download might be redirected to the CDN URL. Ensure that the CDN URL is also allowed if needed.

And make sure that the VM’s have port 443 and port 9443 open.
VM’s use TCP 443 for secure connection and VM replication configuration server use 9443 (this port can be changed).
The logs of the process it saved at a storage account and then stored in a managed disk.
Also download and install the **appliance installer** and after the installation the appliance configuration wizard will launch automatically.

After the appliances have restarted and is set up, go to the **Discover machines** page and finalize the registration.

Now replicate the servers, follow and fill out the fields and start.
You can track and monitor replication while ongoing.

When replication begins you can also run a test migration to see if Azure will migrate successfully.
And then when replication is done we can finally migrate all the selected servers.

Sign in to the appliances when done navigate to **%ProgramData%\ASR\home\svsystems\pushinstallsvc\repository** and find the installers for the OS and versions.
C:\ProgramData\ASR\home\svsystems\bin\genpassphrase.exe -v to view the current passphrase if you forgot from earlier.

Then we will extract the content of the installer tarball to a local folder.
Enter following it the terminal;

```
mkdir /tmp/MobSvcInstaller
tar -C /tmp/MobSvcInstaller -xvf <Installer tarball>
cd /tmp/MobSvcInstaller
```

Then run the installer script;

```
sudo ./install -r MS -v VmWare -q
```

Register the agent with the replication appliances;

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <replication appliance IP address> -P <Passphrase File Path>
```

Finally everthing is done and we have a complete copy of the On-prem servers.

If you have large amount of data you can also use a Microsoft service called Storage boxes. You create a job on the service in Azure, Microsoft then sends a physical disk you copy data to and encrypt with BitLocker and the key is uploaded to the job securely in Azure.
The service supports up to 800TB.