**DR Reference and Recommendations**

Table of Contents

[1. Document History 2](#_Toc150256093)

[2. Application Non-Technical Details 2](#_Toc150256094)

[3. Business Contacts 4](#_Toc150256095)

[4. Migration Personnel 4](#_Toc150256096)

[5. Legacy Solution 5](#_Toc150256097)

[5.1 Architecture Overview 5](#_Toc150256098)

[5.2 Short description 5](#_Toc150256099)

[5.3 Technical Details 5](#_Toc150256100)

[6. New Azure Solution 10](#_Toc150256101)

[6.1 High-Level Architecture 10](#_Toc150256102)

[6.2 Technical Details 11](#_Toc150256103)

[6.2.1 Application Tier 11](#_Toc150256104)

[6.2.2 Data Tier 11](#_Toc150256105)

[6.2.3 Network Security Groups – Inbound Rules 12](#_Toc150256106)

[6.2.4 Network Security Groups – Outbound Rules 12](#_Toc150256107)

[6.3 Backup and Restore 13](#_Toc150256108)

[6.3.1 Database Tier 13](#_Toc150256109)

[6.4 Monitoring and Alerting 13](#_Toc150256110)

[7. Migration Activities 13](#_Toc150256111)

[7.1 Pre-migration activities 13](#_Toc150256112)

[7.2 Migration activities 13](#_Toc150256113)

[7.3 Cut-over Activities. 13](#_Toc150256114)

[7.4 Post-Migration activities 13](#_Toc150256115)

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Change | Author |
| 0.1 | 24.11.2023 | Initial Draft | Bidyendu Dey |
| 0.2 | 28.11.2023 | Detailed information | Bidyendu Dey |
|  |  |  |  |
|  |  |  |  |

# 

# Application Non-Technical Details

|  |  |
| --- | --- |
| Technical Contact Persons: Kjell Einar |  |
| Application ID : |  |
| Business Area : |  |
| Cost allocation code (WBS): |  |
| Business Critical: |  |
| Operational Unit: |  |
| Product Owner: Marthe Elin Hetland |  |

# Business Contacts

|  |  |  |  |
| --- | --- | --- | --- |
|  | GASSCO | Vendor | GASSCO |
|  |  |  |  |
|  |  |  |  |

# Legacy Solution

## Architecture Overview

A diagram of a software application

Description automatically generated

A diagram of a network

Description automatically generated

## Short description

**GBS (Gassco Booking System)**  
  
GBS is a web application developed by for Gassco.

Purchase and sale of capacity in the Norwegian gas transportation system is done in GBS. Most of the business logic and work processes are regulated in various Transport agreements (Terms and Conditions).

GBS is a business critical 24/7 application with high requirements to uptime and response. There are internal and external users, and both authentication and signing are done using requests to the external companies Signicat and Buypass.

GBS Database hosted in Oracle Exadata Appliances at Onpremise.

GBS supports the following business processes:

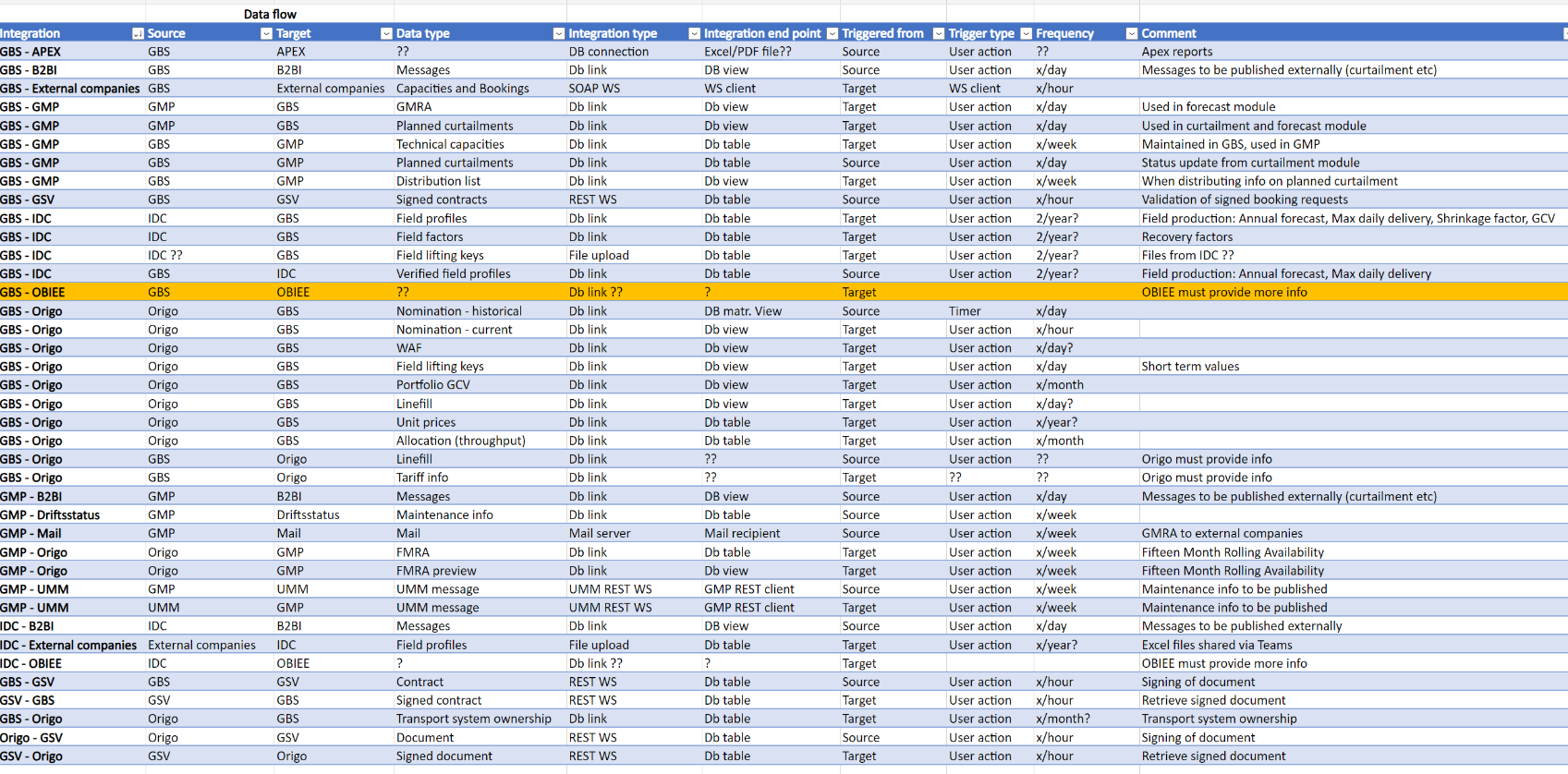
* Booking and rebooking of capacities in primary market
* Purchase and sale of capacity in secondary market
* Capacity overview
* Removal cost obligations
* Curtailment and bottleneck handling
* Booking rounds and allocation of capacities
* Handling of interruptible capacities
* SEGAL
* Company guarantee calculations
* DSRN / capacity need calculations
* Webservice

## Technical Details

Fill in relevant questions and answers from Essential’s questionnaire.

|  |  |
| --- | --- |
| Application Architecture |  |
| Application tier architecture;  Single/Two Tier / Three Tier / N-Tier/Monolith/Distributed? Tier 1 (highly important, 24x7 mission-critical) Tier 2 (moderately important) Tier 3 (low importance, dev/test) | Two Tier Application    Low |
| What is the RPO? | 30min |
| What is the RTO? | 4 |
| What is the technology stack of the application with version? (Programming Language, Framework,Runtime,middleware..etc) | Angular, IBM Weblogic, Rest API for Application Integrations, Oracle DB Links for Database |
| Does the hosting location of this application have an impact on user experience?  i.e. is there a requirement to locate in close proximity to the user base? If yes please provide details in comments section | No. Hosting location at Bygenes and DR at RK. |
| How is the Application accessed? (Eg: Web browser,Thick client, Citrix, Mobile, Multiple) | Web Browser using Bypass Authentication. |
| What is the URL of the application? | gbs.gassco.no |
| What are the present scalability requirements of the application? (Load Balancers, Multiple AppServers etc) | Load Balancer, Multiple App Server & Oracle Database hosted in EXADATA Cluster |
| What is the current application authentication mechanism in place? | IBM LDAP Authentication |
| Deployed manually or via automation | NO |

|  |  |
| --- | --- |
| Infrastructure Information |  |
| Is the application running on a virtualized platform? If No, can it be virtualized? If not, why? | Yes on VMware Virtual Machine |
| In case the servers cannot be moved out AS-IS, is it possible to re-install this application in a freshly deployed server in the Cloud? | Yes new environment would be provisioned |
| Does this application have any stringent network latency requirements? Does latency impact end-user experience or functions of the application and its modules? For eg. very low latency requirement etc. | NO |
| Does this application have High Availability (HA) Requirements? If Yes how is HA implemented | Yes, HA requirements 99.99% in Azure - ?? |
| Does this application require a DR? If YES, how is DR Implemented? What kind of DR - HOT/ Warm/ Cold, Replication strategy, Stretched cluster etc.… | Yes, HA requirements 99.99% in Azure - ?? |
| Does the application need clustering using shared storage? Provide details on Database cluster solution (Ex: Exadata) | No shared storage needed. Oracle Cluster needed |
| Does the application is dependent on any shared infrastructure services? If yes, please provide the details in comments section | NA |
| Does this application have any hardware requirements? For eg. Hardware Key / Hardware License Dependency / Dongle etc? | NA |
| Are there any restriction of licenses for the application to move to cloud? | No. Gassco developed application. |



|  |  |
| --- | --- |
| Platform Information |  |
| Server name |  |
| Number of CPUs |  |
| Memory size |  |
| Capacity of disks |  |
| Dynamic volumes |  |
| C: Content |  |
| E: Content |  |
| F: Content |  |
| G: Content |  |
| H: Content |  |
| OS |  |
| OS Update level |  |

|  |  |
| --- | --- |
| Platform Information |  |
| IP Address: |  |
| Subnet Mask: |  |
| Default Gateway: |  |
| Primary DNS Server: |  |
| Secondary DNS Server: |  |
| TTL Values |  |
| specific DNS servers |  |
| Mac Address: |  |
| Joined to which domain |  |
| Host file modifications (static entries) |  |
| VLAN |  |
| VPN connections |  |

|  |  |
| --- | --- |
| Database Information |  |
| Oracle |  |
| Enter the Release and Version Number, Edition, Patch, Service Pack |  |
| Enter the DB & Application for Shared/Dedicated |  |
| Enter the Database or Instance name(s) associated with this application |  |
| What is the size of your database? |  |
| How many schemas do you have? |  |
| How many big tables do you have (200 gigabytes or 200 million rows in size)? |  |
| What do the transaction boundaries look like? |  |
| Do you have engine-specific data types that won’t be migrated by your migration tool? |  |
| How hot (busy) is your source database? |  |
| What kind of users, roles, and permissions do you have on the source database? |  |
| When was the last time you vacuumed, or compacted, your database? |  |
| How can your database be accessed (firewalls, tunnels, VPNs)? |  |
| Can you afford downtime? How much? |  |
| Do you need the source database to stay alive after the migration? For how long? |  |
| Do you know why you preferred one target database engine over another? |  |
| What are your high availability (HA) requirements? |  |
| Does all the data need to move? |  |
| Does it need to move to the same place? |  |
| Logins with hashed passwords or an SIDs |  |
| Jobs with owner accounts (including SIDs) |  |
| Server configuration settings | AS-IS |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application Firewall Rules |  |  |  |  |
| Initiator App Group / Server Name / IP Address | **Target App Group / Server Name / IP Address** | **PORT** | **Firewall** | **Comments** |
| Inbound/outbound |  |  |  |  |
| Inbound/outbound |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# New Azure Solution

## High-Level Application Architecture

GBS Application to be modernize in Azure. Target Application design to be decided by 2024.

## Technical Details

**Platform (IaaS/PaaS) –**

**Resource groups -**

**Subscription -**

### Application Tier

|  |  |
| --- | --- |
| Platform Information – Application Tier |  |
| Virtual Machine Name |  |
| Image |  |
| VM Size |  |
| Location |  |
| VirtualNetworkName |  |
| SubnetName |  |
| SecurityGroupName |  |
| PublicIpAddressName |  |
| Disks |  |
| OS |  |
|  |  |
| IP Address: |  |
| Subnet Mask: |  |
| Default Gateway: |  |
| Primary DNS Server: |  |
| Secondary DNS Server: |  |
| TTL Values |  |
| specific DNS servers |  |
| Mac Address: |  |
| Joined to which domain |  |
| Host file modifications (static entries) |  |

### Data Tier

|  |  |
| --- | --- |
| Platform Information – Data tier |  |
| Database service |  |
| Server version |  |
| Database instance |  |
| Database size |  |
| Compute tier |  |
| Service tier |  |
| Dymamic scalability |  |
| Security |  |
| Backup retention |  |
| Pricing tier |  |
| Location |  |
|  |  |

A diagram of a diagram

Description automatically generated

### Network Security Groups – Inbound Rules

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Priority | Name | Port/Protocol | Source | Destination | Action |
| 65000 | AllowVnetInBound | Any/Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBound | Any/Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInbound | Any/Any | Any | Any | Deny |

### Network Security Groups – Outbound Rules

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Priority | Name | Port/Protocol | Source | Destination | Action |
| 65000 | AllowVnetOutBound | Any/Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowInternetOutBound | Any/Any | Any | Internet | Allow |
| 65500 | DenyAllOutbound | Any/Any | Any | Any | Deny |

## Backup and Restore

### Database Tier

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Active | Weeks kept | Comment |
| Weekly | Yes |  |  |
| Monthly | Yes |  |  |
| Yearly | No |  |  |

## Monitoring and Alerting

# Tools for Disaster Recovery, on-prem to Azure

1. **Background**

As part of the project we have been looking into how Gassco could do an disaster recovery to Azure, and what tools would suit the task best. During this POC an VM was selected (Hyttebooking) and was successfully restored in Azure using the tools and procedures you can find below.

1. **CAF recommendations**

CAF only refer to Cloud, and DR in a cloud scenario. Here you can read Microsoft’s design considerations and recommendations for a cloud scenario.

1. **Design considerations**

Consider the following factors when designing Business continuity and disaster recovery (BCDR) for application workloads:

* Application and data availability requirements:
* RTO and RPO requirements for each workload.
* Support for active-active and active-passive availability patterns.
* BCDR as a service for platform-as-a-service (PaaS) services:
* Native DR and high-availability (HA) feature support.
* Geo-replication and DR capabilities for PaaS services.
* Support for multiregion deployments for failover, with component proximity for performance.
* Application operations with reduced functionality or degraded performance during an outage.
* Workload suitability for Availability Zones or availability sets:
* Data sharing and dependencies between zones.
* Availability Zones compared to availability sets impact on update domains.
* Percentage of workloads that can be under maintenance simultaneously.
* Availability Zones support for specific virtual machine (VM) stock-keeping units (SKUs). For example, Azure Ultra Disk Storage requires using Availability Zones.
* Consistent backups for applications and data:
* VM snapshots.
* Azure Backup Recovery Services vaults.
* Subscription limits restricting the number of Recovery Services vaults and the size of each vault.
* Network connectivity if a failover occurs:
* Bandwidth capacity planning for Azure ExpressRoute.
* Traffic routing during a regional, zonal, or network outage.
* Planned and unplanned failovers:
* IP address consistency requirements, and the potential need to maintain IP addresses after failover and failback.
* Maintaining engineering DevOps capabilities.
* Azure Key Vault DR for application keys, certificates, and secrets.

1. **Design recommendations**

The following design practices support Business Continuity Disaster Recovery (BCDR) for application workloads:

* Employ Azure Site Recovery for Azure-to-Azure VM DR scenarios.

Site Recovery uses real-time replication and recovery automation to replicate workloads across regions. Built-in platform capabilities for VM workloads meet low RPO and RTO requirements. You can use Site Recovery to run recovery drills without affecting production workloads. You can also use Azure Policy to enable replication and to audit VM protection.

* Use native PaaS DR capabilities.

Built-in PaaS features simplify both design and deployment automation for replication and failover in workload architectures. Organizations that define service standards can also audit and enforce the service configuration through Azure Policy.

* Use Azure-native backup capabilities.

Azure Backup and PaaS-native backup features remove the need for third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy to ensure compliance with organization requirements.

* Use multiple regions and peering locations for ExpressRoute connectivity.

A redundant hybrid network architecture can help ensure uninterrupted cross-premises connectivity if an outage affects an Azure region or peering provider location.

* Avoid using overlapping IP address ranges in production and DR networks.

Production and DR networks that have overlapping IP addresses require a failover process that can complicate and delay application failover. When possible, plan for a BCDR network architecture that provides concurrent connectivity to all sites.

1. **Gassco Tools for DR**

Gasco widely uses Veeam software for backup and recovery management. Veeam Backup & Replication Console is the tool used, and here you should be able to find all backups as well as inventory for tape backup. There is separate Veaam instances for each security zone.

For Gassco it’s therefore natural to find the best way to restore continuing using Veeam, which already have the overview of and contains/maintains all backups in Gassco. A manual method is also natural to test, for the sake of comparison.

1. **Test Restore Report**
2. Summary

To gain experience and confidence in our restore capabilities using Azure, we decided to perform a test restore of an on-premises VM. Our VM of choice was **byhyttep01**. This VM is a small, fairly generic system that hosts an old cabin booking application.

 Attempts were made using two methods:

1. Basic Veeam **Restore VM to Azure** functionality

* With no additional helper appliances, Veeam restores the VM disks to a public endpoint through our proxy/Internet connection. This requires a fairly large list of URLs to be allowed and exempted from inspection through our network proxy.
* Requires a service principal with permissions in Azure to create VMs and related resources.
* **Restore took ca. 11 hours. (60GB)**

1. Manual restore using AzCopy

* VM disks were converted to VHD format using Veeam and sized appropriately using PowerShell cmdlets according to Azure disk size requirements.
* **AzCopy** was used for uploading disk file to private endpoint, thus using our ExpressRoute circuit.
* **Restore took ca. 2 hours. (60GB)**

Both approaches have their pros and cons, but it is preferable to use our private network both for the sake of speed and security. This comes with a cost of additional targeting & configuration requirements though.

Further technical details are laid out in the chapters below.

1. Method 1: Basic Veeam restore to Azure

To restore, the following [official documentation](https://helpcenter.veeam.com/docs/backup/vsphere/restore_azure.html?ver=120) from Veeam was used. The documentation also gives insight into limitations and the some of the technical details and requirements regarding the restore process

1. *Prerequisites and assumptions*

* Basically, this [article](https://helpcenter.veeam.com/docs/backup/vsphere/restore_azure_setup.html?ver=120) from Veeam was followed to give Veeam a foothold within our Azure tenant.
* Details in CRQ000000054132.
* Required network openings are listed in the table below which were obtained through Veeam’s network [guide](https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html?ver=120), Microsoft’s [overview](https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide) and test sessions where we continuously opened observed necessary observed traffic.
* Proxy details in CRQ000000054130
* Firewall details in CRQ000000054129 and CRQ000000054128
* Required Azure subscription for testing created - CRQ000000053757
* Required private virtual network and subnets created - CRQ000000053926
* Required authorization is available to obtain backups from Veeam and create necessary resources in Azure.
* Restoration was performed using backup from disk repository to save some time. Restore from tape functionality was assumed to be in working condition.

1. *Walkthrough*

* Connect to the Veeam backup server (**byveeamp01** in this case) using Remote Desktop.
* Open the **Veeam Backup & Replication** console
* Select **Backups** and use the search field to find the VM to restore, in our case **byhyttep01**.
* Right-click the newest created backup stored on the **BYFSBP02** repository and select **Restore to Microsoft Azure…**
* Select the correct subscription (Gassco-DisasterRecovery-Test) and location (West Europe)
* Skip selecting a proxy appliance. It will automatically use **byveeamp01** for restoration since there is no helper appliance in Azure. A helper appliance would increase restore speed, but it requires additional setup.
* Select a name - **gcwehyttep01**
* Do not select a storage account – confirm the prompt for using Managed Disks.
* Select size – **Standard\_B2s\_v2**
* Select Resource Group – **gcwehyttebooking**
* Select existing virtual network – **gcwedrvnett01**
* Select existing subnet – **WindowsVMs**
* Select existing security group (NSG) – **WindowsVMs-nsg**
* Important: Turn off public IP!
* Start the restoration and wait. Took 11 hours when I did it.
* Once successful, connect to **byazuremgmtp01** using Remote Desktop.
* Use Remote Desktop to connect to the VM private IP address. Obtain the corresponding LAPS password from on-premise AD to authenticate with since the VM is most likely unable to use domain logon. Use **.\glaps** as username when connecting.
* To obtain LAPS password: Log on to a domain controller, open **LAPS UI** (as admin!) and search for the server password.

1. Method 2: Manual restore/disk upload using AzCopy

Azure VMs basically run on a customized Hyper-V platform. For VMware VMs to be able to run on the Azure platform, one can convert VMDK disk files from VMware over to VHD/VHDX which is the Hyper-V disk format.  This conversion can be done with Veeam disk export and some manual cmdlets in Powershell.

There are some considerations to know about, especially important is disk sizing, which can be found in this [article](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image) from Microsoft.

After getting VHD files from Veeam, this [article](https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disks-upload-vhd-to-managed-disk-cli) was used for the creation of disk resources & upload steps.

1. *Prerequisites and assumptions*

* We have an available backup within Veeam which can be exported for use.
* Required Azure subscription for testing created - CRQ000000053757
* Required private virtual network and subnets created - CRQ000000053926
* HTTPS (TCP 443) and RDP (TCP 3389) is open towards the subnet in Azure that will host the restored VM and its corresponding managed disks, from an upload server on-premises. (**byazuremgmtp01)**
* Required authorization is available to obtain backups from Veeam and create necessary resources in Azure.
* Azure CLI is available on the upload server (**byazuremgmtp01)**
* Hyper-V feature is installed on Veeam repository server in order to use VHD resizing cmdlets/tools.
* AzCopy tool is available on upload server (**byazuremgmtp01)**

1. *Walkthrough*

* Connect to the Veeam server, **byveeamp01** in this case, using your admin account and Remote Desktop.
* Open the **Veeam Backup & Replication** console.
* Select **Backups** and use the search field to find the VM in question.
* Right-click the backup from the **BYFSBP02** repository and select **Export content as virtual disks…**
* Click **Next** until you arrive at the **Target** section.
* Select **byfsbp02** as the target server and select folder on a drive with enough space.
* Select **VHD** as export format.
* Select **Fixed** as Disk type.
* Continue
* Click **Next** until the export/restore is started.

Now that you have Hyper-V compatible VM disks, you must convert them to a size that is compatible with Azure. Disks in Azure must be aligned to 1MiB. The file size also requires 512 bytes for the VHD footer.

* Connect to the Veeam repository server, **byfsbp02** in this case, using your admin account and Remote Desktop
* Open PowerShell (Admin)
* Find the current size of the VM using **Get-VHD** against the VHD file(s).
* Increase the size slightly using **Resize-VHD**. Ensure that the new size is aligned to 1MB
* To test this, run this fraction command: **<size\_in\_bytes> % 1MB**. The resulting bytes value should be 0.
* After resizing, you can confirm this by validating **FileSize** and **Size** values from **Get-VHD**
* The **FileSize** value, when checked with **<size\_in\_bytes> % 1MB**, should give 512 as result.
* The **Size** value, when checked with **<size\_in\_bytes % 1MB**, should give 0 as result.
* Copy the disk files to a secure location where they can be reached from **byazuremgmtp01**, such as **byfsap01\e$\temp**

Now you have available VM disk files which can be used for the upload step with AzCopy. However, first, empty disk resources must be created in Azure that will take receive them.

* Connect to byazuremgmtp01 with an admin account with appropriate Azure permissions using Remote Desktop.
* Open the Azure Portal using a web browserand navigate to the **Gassco-DisasterRecovery-Test** subscription.
* Create a resource group if not already there: **gcwehyttebooking**
* In the resource group, add a **Data Access** resource. This is required for upload to the disk resources via private endpoint.
* During this creation, ensure to create a private endpoint & network interface in the **WindowsVMs** subnet.
* Open a CMD/PowerShell prompt and use **az login** to connect to Azure Resource Manager.
* Use the following command to create managed disks as necessary that are ready to receive uploaded content through data access / private endpoint:
* *az disk create -n* ***<new disk name>*** *-g gcwehyttebooking -l westeurope --os-type Windows --upload-type Upload --upload-size-bytes* ***<VHD filesize>*** *--sku standard\_lrs --hyper-v-generation v1 --disk-access* ***<disk-access-resource-name>***
* Must use Hyper-V Generation 1 for VHD format disks
* Must use Hyper-V Generation 1 when using BIOS instead of UEFI
* Grant temporary access token (SAS) URI using Azure CLI. Store the URL given in output for use with AzCopy later
* *az disk grant-access -n* ***<new disk name>*** *-g gcwehyttebooking --access-level Write --duration-in-seconds 86400*
* Upload with AzCopy:
* *azcopy.exe* ***<VHD file/network-path>******<SAS URI>*** *--blob-type PageBlob*
* Once disk upload is complete, revoke access and make the disk usable with Azure CLI:
* *az disk revoke-access -n* ***<new disk name>*** *-g gcwehyttebooking*
* Open the Azure Portal in your web browser and find the new managed disk resources below the **gcwehyttebooking**. Select **Create VM**
* You will be asked about a **lot** of parameters regarding the VM. For this test, cheap sizing and low redundancy choices were made to save costs.
* Basics
* Provide a name in the format **gcwe<name><p/t/d><number>, e.g. gcwehyttep01**
* Location = West Europe
* Availability options = No infrastructure redundancy required
* Security type = Standard
* Image = <managed disk>
* Size = Standard\_B2s
* Public inbound ports = None
* License type = Windows server
* Disks
* OS disk type = Standard SSD
* Delete with VM = Yes
* (Optional) Data disks = Attach an existing disk
* Add additional uploaded disks here as necessary that are related to the VM.
* Virtual network = gcwedrnett01
* Subnet = WindowsVMs
* Public IP = None
* NIC network security group = Advanced
* WindowsVMs-nsg
* Delete NIC when VM is deleted = Yes
* Management
* Turn off automatic updates.
* Monitoring
* Leave as is
* Advanced
* Leave as is
* Tags
* Add **managedBy =** [**cloudplatform@gassco.no**](mailto:cloudplatform@gassco.no) or what is appropriate
* Finish with **Review + create**

The VM should now be provisioned. You will want to validate the IP address and add it, with its MAC address to our IPDB:

* Find the VM NIC in the **gcwehyttebooking** resource group. Open **Properties** on the left and note the MAC address.
* Open **IP configurations** on the right and ensure the private IP address is appropriate. Take note of it and add it to our IPDB.

A screenshot of a computer

Description automatically generated

*Figure 1: Example of resources related to VM (VM, disk access/private endpoint/NIC, managed disks and VM NIC)*

Now that you have the VM IP address, you should be able to connect using Remote Desktop from byazuremgmtp01:

* Use Remote Desktop to connect to the VM private IP address. Obtain the corresponding LAPS password from on-premise AD to authenticate with since the VM is most likely unable to use domain logon. Use **.\glaps** as username when connecting.
* To obtain LAPS password: Log on to a domain controller, open **LAPS UI** (as admin!) and search for the server password.

1. Troubleshooting and other notes/observations

* The **Boot Diagnostics** section on the Azure VM resource will show you a screenshot from the VM console which refreshes once in a while.
* First attempt at restore failed due to an old, unmaintained Ivanti driver causing a BSOD when transitioned from VMware to Hyper-V/Azure. This was resolved by renaming the driver file (**cismbios.sys** below C:\Windows\System32\Drivers) before a new upload attempt to Azure. This was achieved by mounting the VHD file in File Explorer and editing there directly.
* Azure does *not* have a normal VM console available for VMs which makes troubleshooting boot issues and similar problems bothersome.
* There is an Azure serial console, but this is not available immediately after restore from on-prem unless prerequisites are in place, which are yet to be researched.
* Azure does *not* grant the ability to edit content in managed disks, making it difficult to fix boot issues via file editing on the drives themselves.
* Azure uses Hyper-V. Having a little bit of Hyper-V on-premises for compatibility/testing can be beneficial.
* If interested in mass migration, there are other options to consider, such as **Azure Migrate,** that may prove faster when some setup requirements are met.
* The restored server is not able to connect to Domain controller or have any other outbound connection for that matter. In a future DR-scenario, there is work related to network/infrastructure that would need to be done to get the DR server operational. For Gassco to be ready for a DR-scenario, Gassco could prepare Azure for DR-scenario having a prepared landing zone on stand-by ready to receive and connect recovered servers.