POC Re-host sample workload from on-premises to cloud (use CAF methodology)

Table of Contents

[1. Executive Summary 4](#_Toc154064518)

[2. Introduction 4](#_Toc154064519)

[3. About the sample application 4](#_Toc154064520)

[4. Discovery & assessment 5](#_Toc154064521)

[4.1 Discovery of Applications 5](#_Toc154064522)

[4.2 Cloud Compatibility & Migration Readiness Assessment 5](#_Toc154064523)

[5. CAF on Azure migration 5](#_Toc154064524)

[6. Gassco environment 5](#_Toc154064525)

[7. Tools for management of VM’s in Azure Landingzones 6](#_Toc154064526)

[7.1 Background 6](#_Toc154064527)

[7.2 Scope 6](#_Toc154064528)

[7.3 Key Business Areas 6](#_Toc154064529)

[7.4 Tools recommended in caf: 6](#_Toc154064530)

[7.4.1 CAF Management Baseline Inventory and visibility 6](#_Toc154064531)

[7.4.2 CAF Management Baseline Operational Management 7](#_Toc154064532)

[7.4.3 CAF Management Baseline Protect and recover 7](#_Toc154064533)

[7.5 On-prem tools 7](#_Toc154064534)

[7.5.1 On-prem 7](#_Toc154064535)

[7.5.2 Gassco on-prem Inventory and visibility 8](#_Toc154064536)

[7.5.3 Gasso on-prem Operational Management 8](#_Toc154064537)

[7.5.4 Gassco on-prem Protect and recover 8](#_Toc154064538)

[7.5.5 On-prem metrics and monitoring 9](#_Toc154064539)

[7.6 The way forward 9](#_Toc154064540)

[7.6.1 Tools for VM landing zone 9](#_Toc154064541)

[7.6.2 Gassco Baseline Inventory and visibility 9](#_Toc154064542)

[7.6.3 Gassco Management Baseline Operational Management 10](#_Toc154064543)

[7.6.4 Gassco Management Baseline Protect and recover 10](#_Toc154064544)

[7.6.5 Splunk integration 10](#_Toc154064545)

[7.7 Internal Security Approval 11](#_Toc154064546)

[7.7.1 Getting started security approval 11](#_Toc154064547)

[8. Rehost Hyttebooking on Azure 11](#_Toc154064548)

[8.1 Key takeaways 11](#_Toc154064549)

[9. Tools for Disaster Recovery, on-prem to Azure 12](#_Toc154064550)

[9.1 Background 12](#_Toc154064551)

[9.2 CAF recommendations 12](#_Toc154064552)

[9.2.1 Design considerations 12](#_Toc154064553)

[9.2.2 Design recommendations 12](#_Toc154064554)

[9.3 Gassco Tools for DR 13](#_Toc154064555)

[9.3.1 Test Restore Report 13](#_Toc154064556)

[9.4 Conclusion 18](#_Toc154064557)

[9.4.1 Key takeaways 18](#_Toc154064558)

[10. Azure Policies 18](#_Toc154064559)

[10.1.1 Design Considerations 18](#_Toc154064560)

[10.1.2 Design Recommendations 18](#_Toc154064561)

[10.1.3 Solution Architecture 19](#_Toc154064562)

[10.2 Optional Azure Policies 20](#_Toc154064563)

# Executive Summary

As part of the ongoing Cloud project, there was an interest in researching what could be done regarding disaster recovery and potentially running on-prem workloads in the cloud. On this specific track we wanted to explore how to rehost the identified application, leveraging cloud capabilities to enhance scalability, flexibility, and overall performance.

There were several blockers for us to fully explore all initial queries, one was time limitation, others of strategic and technical matter. For instance there is as of now a policy of not establishing an AD DS in Azure, and restrictions regarding network connections. This hinders us to realistically test all aspects with a workload moved to cloud. This needs to be addressed before or as part of an future migration project, or else this will also block migrating the majority of on-prem workloads to the cloud.

In Gassco there is a decision to reference and if possible follow Microsoft’s Cloud Adaption Framework (CAF) for the cloud adoption. In this specific case CAF will recommend the organization to develop their own migration strategy, given they have some specific policies applied in the organization. This is definitely required for Gassco, and there should be an initiative to develop a holistic cloud migration approach setting the premise for future migrations and preventing major blockers (as mentioned earlier) for a cloud transition.

We explored what tools could be used managing workloads in cloud, also what tools Gassco uses on-prem and what requirements there where to survey different parameters on the infrastructure. Resulting in a possible future recommendation of cloud tools with on-prem integration so the surveillance can be tracked/reported in known tools for Gassco operations. Also there is a section recommending specific Azure Policies, an Azure Policy enforces rules and effects over resources, to stay compliant with Gassco’s corporate standards. Other policies should be considered in a future migration project.

In short this is what has been explored and what you can read about in more detail in this report.

# Introduction

In this exercise «Hyttebooking» is chosen to be the target app for an migration scenario. Preferably using Microsoft Cloud Adaption Framework (CAF) how could Gassco migrate workloads to the cloud. There is many ways of migrating applications to the cloud, both what type of tool you utilize and methodology. Those workloads could be moved to the cloud through any number of approaches: lift and shift, lift and optimize, or modernize. Each approach is considered a migration. For each workload there should be a pre study of which approach is suitable, for some workloads lift an shift will be and quick and easy way of moving to the cloud, for other applications modernise is a must because of legacy solution or technologies. In any case optimization of workload is recommended when moved to cloud, like optimizing when lift and shift is done, or use a lift and optimize approach optimizing in the process.

# About the sample application

Hyttebooking is a small custom in-house app accessed thru web, for its users to book cabins in connection to vacation or company outings. It has a small footprint using just one application server (byhyttep01) with the application and it has SQL database on the Large SQL server cluster. The application is built using .NET, and it uses the AD to authenticate the users.

# Discovery & assessment

## **Discovery of Applications**

In order to understand the target applications we have reach out to Business Unit head or Group Lead to understand the application or portfolio of applications. Then we performed an high Level assessment for in-scope applications & did dependency mapping. Then we went ahead with an detailed Cloud Assessment.

## **Cloud Compatibility & Migration Readiness Assessment**

During the assessment we performed a manual application assessment via questionnaires. Conducted Workshops with application owners to capture complete snapshot & validate integrations / dependencies. Captured performance matrix of application & database servers. Then provide Cloud Readiness output, to decide on the migration approach to decide right “R”.

# CAF on Azure migration

There is a section about migration in CAF, you will find it [here](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-migration-guide/). Where they have a section about when to use the CAF migration guide, following here:

***When to use this guide***

*The tools discussed in this guide support various migration scenarios. You can use this guide as a baseline for most migrations, and this format works well for planning and migrating most workloads.*

*To determine whether this migration guide is suitable for your project, consider whether the following conditions apply to your situation:*

* *The workloads for initial migration aren't mission-critical and don't contain sensitive data.*
* *You're migrating a homogeneous environment.*
* *Only a few business units need to align to complete the migration.*
* *You're not planning to automate the entire migration.*
* *You're migrating a small number of servers.*
* *The dependency mapping of the components to be migrated is simple to define.*
* *Your industry has minimal regulatory requirements relevant to this migration.*

Based on this, Gassco can only reference CAF for migrating workloads, but need to develop and own their own way of migrating workloads to the cloud. Some workloads may be migrated using more or less the tools and procedures listed in CAF, others will need their own approach. This needs to be detailed in a separate migration project. There are also need of a clear (holistic) migration strategy at Gassco, not if we move to cloud, but what to do when. This should detail all common areas like IAM, especially for migrated on-prem workloads who need’s a AD to authenticate users. Detail around security requirements, network, tools and shared resources. Some of this is explored in this task.

# Gassco environment

Today Gassco run servers in their own datacenter, mainly on VMware. It’s possible to keep running servers on VMware in Azure, with “Azure VMware Solution”, or run an hybrid scenario. But to be able to utilize Azure cloud fully, especially for Windows servers and MS-SQL, migrating workloads and running these as virtual machines in Azure will in most cases be the best option, possibly combined with Azure SQL Database (PaaS)

# Tools for management of VM’s in Azure Landingzones

## Background

This section will describe the necessary tooling and routines managing and running services in cloud environment (Azure).

Referencing CAF and evaluating the tool’s used at Gassco today, will result in an recommendation going forward, migrating a workload to Azure.

Planning for monitoring and alerts will ensure a secure and stable delivery from cloud, preventing downtime and capacity issues.

## Scope

The scope of this document is limited to the landing zone for VM infrastructure and describing the supporting tools.

## Key Business Areas

As a data platform, Mimir serves several business areas and functions in Gassco. Ranging from financial budgeting services, reporting and effectivization of manual business processes.

## Tools recommended in caf:

A blue sign with black text

Description automatically generated

### CAF Management Baseline Inventory and visibility

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Monitor health of Azure services | [Azure Service Health](https://learn.microsoft.com/en-us/azure/service-health/service-health-overview) | Health, performance, and diagnostics for services running in Azure |
| Log centralization | [Log Analytics](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview) | Central logging for all visibility purposes |
| Monitoring centralization | [Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/overview) | Central monitoring of operational data and trends |
| Virtual machine inventory and change tracking | [Change Tracking and Inventory in Azure Automation](https://learn.microsoft.com/en-us/azure/automation/change-tracking/overview) | Inventory VMs and monitor changes for guest OS level |
| Subscription monitoring | [Azure activity log](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log) | Monitoring change at the subscription level |
| Guest OS monitoring | [Azure Monitor for VMs](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview) | Monitoring changes and performance of VMs |
| Network monitoring | [Azure Network Watcher](https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview) | Monitoring network changes and performance |
| DNS monitoring | [DNS Analytics](https://learn.microsoft.com/en-us/azure/azure-monitor/insights/dns-analytics) | Security, performance, and operations of DNS |

*From* [*Microsoft learn*](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-management-guide/inventory?tabs=AzureServiceHealth%2CLog-Analytics%2CAzure-Monitor%2CConfigure-solutions)

Note:

* Onboard entire subscription to utilize full set of capabilities in Log Analytics ([Configure the service for a subscription - Cloud Adoption Framework | Microsoft Learn](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/onboard-at-scale))

### CAF Management Baseline Operational Management

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Patch management | Azure Automation Update Management | Management and scheduling of updates |
| Policy enforcement | Azure Policy | Policy enforcement to ensure environment and guest compliance |
| Environment configuration | Azure Blueprints | Automated compliance for core services |
| Resource configuration | Desired State Configuration | Automated configuration on guest OS and some aspects of the environment |

### CAF Management Baseline Protect and recover

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Protect data | Azure Backup | Back up data and virtual machines in the cloud. |
| Protect the environment | Microsoft Defender for Cloud | Strengthen security and provide advanced threat protection across your hybrid workloads. |

## On-prem tools

### On-prem

This section describes the on-prem tools and requirements currently in use in Gassco today. These tools and requirements must be taken into consideration when selecting tools for cloud management/operation. Looking into possible integration and reporting to stay in-line with Gassco’s security requirements.

### Gassco on-prem Inventory and visibility

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Monitor health | VMware vCenter  CA Unified Infrastructure Manager | Health, performance, and diagnostics for services |
| Log centralization | Splunk | Central logging for all visibility purposes |
| Monitoring centralization | VMware vCenter VMware Aria Operations  Splunk  CA Unified Infrastructure Manager | Central monitoring of operational data and trends |
| Virtual machine inventory and change tracking | Ivanti Endpoint Manager  VMware vCenter | Inventory VMs and monitor changes for guest OS level |
| Guest OS monitoring | CA Unified Infrastructure Manager  (VMware vCenter)  VMware Aria Operations | Monitoring changes and performance of VMs |
| Network monitoring | VMware Aria Operations VMware vCenter | Monitoring network changes and performance |

### Gasso on-prem Operational Management

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Patch management | Ivanti Endpoint Manager | Management and scheduling of updates |
| Policy enforcement | Windows server GPO Powershell scripts | Policy enforcement to ensure environment and guest compliance |
| Resource configuration | Windows Server GPO  Powershell scripts | Automated configuration on guest OS and some aspects of the environment |

### Gassco on-prem Protect and recover

|  |  |  |
| --- | --- | --- |
| **Process** | **Tool** | **Purpose** |
| Protect data | Veeam Backup & Replication (IBM Spectrum Protect) | Back up data and virtual machines |
| Protect the environment | Symantec Endpoint Protection Manager Sysinternals - Sysmon Tenable Security Center (Nessus) | Strengthen security and provide advanced threat protection across your hybrid workloads. |

### On-prem metrics and monitoring

|  |  |  |  |
| --- | --- | --- | --- |
| **Metrics** | **Monitored** | **Required** | **Tool** |
| CPU | Yes | No | CA Unified Infrastructure Manager (CAUIM) VMware Aria Operations |
| Memory | Yes | No | CA Unified Infrastructure Manager (CAUIM) VMware Aria Operations |
| Disk capacity | Yes | No | CA Unified Infrastructure Manager (CAUIM) VMware Aria Operations |
| Disk load | Yes | No | VMware Aria Operations |
| Patch | Yes | Yes | Ivanti Endpoint Manager (Tenable Security Center) |
| AV status | Yes | Yes | Symantec Endpoint Protection Manager & Splunk |
| Downtime | Yes | Yes | CA Unified Infrastructure Manager (CAUIM) |
| Network/NIC | Yes | No | VMware Aria Operations |

## The way forward

### Tools for VM landing zone

This section describes the tools that is recommended for Gassco moving forward with VM landing zones in Azure. Also considering existing on-prem tools and integrations to make operational tasks easier integrating with centralized incident tools. With no integration, the current operations team must handle on-prem and cloud separately, or there needs to be an separate team handling cloud until there is a formal process for handling incidents in cloud environment.

### Gassco Baseline Inventory and visibility

|  |  |  |  |
| --- | --- | --- | --- |
| **Process** | **Tool** | **Purpose** | **Comment** |
| Monitor health of Azure services | [Azure Service Health](https://learn.microsoft.com/en-us/azure/service-health/service-health-overview) | Health, performance, and diagnostics for services running in Azure |  |
| Log centralization | [Log Analytics](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview) | Central logging for all visibility purposes | Splunk integration |
| Monitoring centralization | [Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/overview) | Central monitoring of operational data and trends | Splunk integration |
|  |  |  |  |
| Virtual machine inventory and change tracking | [Change Tracking and Inventory in Azure Automation](https://learn.microsoft.com/en-us/azure/automation/change-tracking/overview) | Inventory VMs and monitor changes for guest OS level |  |
| Subscription monitoring | [Azure activity log](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log) | Monitoring change at the subscription level |  |
| Guest OS monitoring | [Azure Monitor for VMs](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview) | Monitoring changes and performance of VMs |  |
| Network monitoring | [Azure Network Watcher](https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview) | Monitoring network changes and performance |  |
| DNS monitoring | [DNS Analytics](https://learn.microsoft.com/en-us/azure/azure-monitor/insights/dns-analytics) | Security, performance, and operations of DNS | KIS: Unlikely to be necessary? |

### Gassco Management Baseline Operational Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Process** | **Tool** | **Purpose** | **Comment** |
| Patch management | Azure Automation Update Management | Management and scheduling of updates |  |
| Policy enforcement | Azure Policy | Policy enforcement to ensure environment and guest compliance |  |
| Environment configuration | Azure Blueprints | Automated compliance for core services |  |
| Resource configuration | Desired State Configuration | Automated configuration on guest OS and some aspects of the environment | Not likely that we want to |

### Gassco Management Baseline Protect and recover

|  |  |  |  |
| --- | --- | --- | --- |
| **Process** | **Tool** | **Purpose** | **Comment** |
| Protect data | Azure Backup | Back up data and virtual machines in the cloud. |  |
| Protect the environment | Microsoft Defender for Cloud | Strengthen security and provide advanced threat protection across your hybrid workloads. | Splunk integration |

### Splunk integration

Splunk can fetch/receive a number of data from Azure. Focusing here on data from Azure VM’s. For VM’s and other relevant data “Microsoft Azure ad-on for Splunk” and possibly “Splunk Add-on for Microsoft Cloud services” can be used. For a simple overview see the diagram below.

A close-up of a chart

Description automatically generated[Getting Microsoft Azure Data into Splunk | Splunk](https://www.splunk.com/en_us/blog/tips-and-tricks/getting-microsoft-azure-data-into-splunk.html)

## Internal Security Approval

To be able to set tools in production they need to be approved by Gassco Security team.

### Getting started security approval

Write up the reasoning for using the tool. If necessary do a design. Contact Security team for approval.

# Rehost Hyttebooking on Azure

Combined with looking in to DR, in this particular test we used Veeam to restore the VM in Azure. You can read the full report in the [LINK to DOCUMENT]/Or below. In a bigger migration scenario there would be other tools and methods to be used. Azure Migrate is one powerful tool from Microsoft analyzing and migrating workloads. This will also give a cost estimate for a specific workload, and link dependencies in the environment.

Restoration from on-premise to Azure has been proven possible, giving us some experience and confidence about this option should we need to do such a task in the future..

## Key takeaways

* Network speed is the most limiting factor. In order for Azure to be a realistic DR platform, backups/replicas should already be placed there to reduce the time before getting online (Recovery Time Objective)
  + Using our private Azure ExpressRoute link proved to be a lot faster than going through the Internet/proxy.
* There are compatibility considerations to make between the virtualization platforms (VMware and Hyper-V/Azure)
* Restoration should be done with as few middle staging points (e.g. jump servers) as possible for the sake of restoration speed.
* The methods used here can be used for migration of VMs (rehosting), if desirable.

# Tools for Disaster Recovery, on-prem to Azure

## 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. Also looking into if the tools can be used in a migration scenario. During this POC an VM was selected (Hyttebooking) and was successfully restored in Azure using the tools and procedures you can find below.

## 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.

### 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.

### 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.

## 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.

### Test Restore Report

#### 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)**
2. 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.

#### 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

##### 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.

##### 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.

#### 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.

##### 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)**

##### 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.

#### 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.

## Conclusion

Restoration from on-premise to Azure has been proven possible, giving us some experience and confidence about this option should we need to do such a task in the future..

### Key takeaways

* Network speed is the most limiting factor. In order for Azure to be a realistic DR platform, backups/replicas should already be placed there to reduce the time before getting online (Recovery Time Objective)
  + Using our private Azure ExpressRoute link proved to be a lot faster than going through the Internet/proxy.
* There are compatibility considerations to make between the virtualization platforms (VMware and Hyper-V/Azure)
* Restoration should be done with as few middle staging points (e.g. jump servers) as possible for the sake of restoration speed.
* The methods used here can be used for migration of VMs (rehosting), if desirable.

# Azure Policies

An Azure Policy enforces rules and effects over resources, to stay compliant with GASSCO’s corporate standards. Similar policies should be grouped together in an initiative to make intent clearer. For example, one initiative containing all policies regarding tag requirements. Best Practice from Microsoft is not to enforce policies but to audit them and remediate.

### Design Considerations

* Determine what Azure policies are needed.
* Enforce management and security conventions, such as the use of private endpoints.
* Manage and create policy assignments by using policy definitions can be reused at multiple inherited assignment scopes. You can have centralized, baseline policy assignments at management group, subscription, and resource group scopes.
* Ensure continuous compliance with compliance reporting and auditing.
* Understand that Azure Policy has limits, such as the restriction of definitions at any particular scope: [policy limits](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits).
* Understand regulatory compliance policies.

### Design Recommendations

* Identify required Azure tags and use the append policy mode to enforce usage.
* Map regulatory and compliance requirements to Azure Policy definitions and Azure AD RBAC assignments.
* Establish Azure Policy definitions at the top-level root management group so that they can be assigned at inherited scopes.
* Manage policy assignments at the highest appropriate level with exclusions at bottom levels, if required.
* Use Azure Policy to control resource provider registrations at the subscription and/or management group levels.
* Use built-in policies where possible to minimize operational overhead.
* Assign the built-in Policy Contributor role at a particular scope to enable application-level governance.
* Limit the number of Azure Policy assignments made at the root management group scope to avoid managing through exclusions at inherited scopes.

### Solution Architecture

| **Policy** | **Input** | **Assignment Level** |
| --- | --- | --- |
| Blueprint initiative for ISO 27001 / CMMI 4 / Any other | Select All \* |  |
| Allowed locations for resource groups | West Europe |  |
| Allowed Locations | West Europe |  |
| Require specified tag  Append tag and its default value | [**See tagging baseline**](#_Cloud_Direct_Tagging) |  |
| Deploy default Microsoft IaaS Antimalware extension for Windows Server |  |  |
| Deploy Log Analytics Agent for Linux VMs |  |  |
| Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS) |  |  |
| Deploy Log Analytics Agent for Windows VMs |  |  |
| Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS) |  |  |
| Deploy network watcher when virtual networks are created |  |  |
| Diagnostic logs in Virtual Machine Scale Sets should be enabled |  |  |
| Diagnostic logs in Logic Apps should be enabled |  |  |
| Diagnostic logs in Key Vault should be enabled |  |  |
| Diagnostic logs in Event Hub should be enabled |  |  |
| Diagnostic logs in App Services should be enabled |  |  |
| Just-In-Time network access control should be applied on virtual machines |  |  |
| Subnets should be associated with a Network Security Group |  |  |
| Vulnerabilities should be remediated by a Vulnerability Assessment solution |  |  |
| The NSGs rules for web applications on IaaS should be hardened |  |  |
| Vulnerabilities on your SQL databases should be remediated |  |  |
| Deploy requirements to audit Windows VMs that do not have the password complexity setting enabled | \* |  |
| Audit Windows VMs that do not have the password complexity setting enabled |  |  |
| Deploy requirements to audit Linux VMs that allow remote connections from accounts without passwords |  |  |
| Audit Linux VMs that allow remote connections from accounts without passwords |  |  |
| Deploy requirements to audit Linux VMs that have accounts without passwords |  |  |
| Audit Linux VMs that have accounts without passwords |  |  |
| Audit Windows VMs that contain certificates expiring within the specified number of days | 30 days |  |
| Audit Windows VMs with a pending reboot |  |  |

## Optional Azure Policies

| **Policy** | **Input** |
| --- | --- |
| Allowed virtual machine SKUs | Cost and compliance control mechanism |
| Allowed storage account SKUs | Cost and compliance control mechanism |
| Not allowed resource types | For security or cost control |
| Network interfaces should not have public IPs | For specific VNET or Subnets based on req. |
| Deploy SQL DB transparent data encryption |  |
| Deploy Threat Detection on SQL servers |  |
| Enforce automatic OS upgrade with app health checks on VMSS |  |
| Enforce encryption on Data Lake Store accounts |  |
| Require blob encryption for storage accounts |  |
| Audit VMs that do not use managed disks |  |
| Diagnostic logs in IoT Hub should be enabled |  |
| Diagnostic logs in Azure Stream Analytics should be enabled |  |
| Diagnostic logs in Service Bus should be enabled |  |
| Diagnostic logs in Search Services should be enabled |  |
| Diagnostic logs in Azure Data Lake Store should be enabled |  |
| Diagnostic logs in Data Lake Analytics should be enabled |  |
| Diagnostic logs in Batch accounts should be enabled |  |
| Audit Windows VMs that are not set to the specified time zone |  |
| Audit Windows VMs that are not joined to the specified domain |  |
| Audit Windows Server VMs on which Windows Serial Console is not enabled |  |
| Audit Windows VMs that do not contain the specified certificates in Trusted Root |  |