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

Table of Contents

[1. Introduction 3](#_Toc152663363)

[2. About the test application 3](#_Toc152663364)

[3. CAF on Azure migration 3](#_Toc152663365)

[4. Gassco and VMvare 4](#_Toc152663366)

[5. Tools for management of VM’s in Azure Landingzones 4](#_Toc152663367)

[6. Background 4](#_Toc152663368)

[7. Scope 4](#_Toc152663369)

[8. Key Business Areas 4](#_Toc152663370)

[9. Tools recommended in caf: 4](#_Toc152663371)

[9.1 CAF Management Baseline Inventory and visibility 4](#_Toc152663372)

[9.2 CAF Management Baseline Operational Management 5](#_Toc152663373)

[9.3 CAF Management Baseline Protect and recover 5](#_Toc152663374)

[10. On-prem tools 6](#_Toc152663375)

[10.1 On-prem 6](#_Toc152663376)

[10.2 Gassco on-prem Inventory and visibility 6](#_Toc152663377)

[10.3 Gasso on-prem Operational Management 6](#_Toc152663378)

[10.4 Gassco on-prem Protect and recover 7](#_Toc152663379)

[10.5 On-prem metrics and monitoration 7](#_Toc152663380)

[11. The way forward 7](#_Toc152663381)

[11.1 Tools for VM landing zone 7](#_Toc152663382)

[11.2 Gassco Baseline Inventory and visibility 7](#_Toc152663383)

[11.3 Gassco Management Baseline Operational Management 8](#_Toc152663384)

[11.4 Gassco Management Baseline Protect and recover 8](#_Toc152663385)

[11.5 Splunk integration 9](#_Toc152663386)

[12. Internal Security Approval 9](#_Toc152663387)

[12.1 Getting started security approval 9](#_Toc152663388)

# 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 and lift and optimize approach optimizing in the process.

# About the test 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 on the Large SQL server cluster. The application is built using .NET, and it uses the AD to authenticate the user.

# 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/). There 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.*

As you can see 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 an procedures listed in CAF, others will need their own approach.

# Gassco and VMvare

Gassco

# Tools for management of VM’s in Azure Landingzones

# Background

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

Referencing CAF and evaluating the tool in use 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 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 too 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 monitoration

|  |  |  |  |
| --- | --- | --- | --- |
| **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.

## 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.