Infrastructure Design Hyper-V

Barenbrug

Document details	
Version:	1.0
Status:	Approved
Last Updated:	20/01/2021
Author(s):	Radis Nizamutdinov

Contents

1.1 Table of Figures

1.2 Table of Tables

Section A – Infrastructure Design - High Level

2. Introduction

2.1 Document Purpose

This design documents the infrastructure design for Hyper-V.

- It will detail the High level (HLD) elements of design in section A. This section will show solution concepts and provide rationale for design decisions. It will also contain the Bill of Materials.
- It will detail the Low level (LLD) elements of design in section B. The section will provide sufficient information to enable the infrastructure to be built, as no associated build documentation will be created.

2.2 Scope & Requirements Traceability

2.2.1 Requirements Traceability

No specific requirements have been provided. The following requirements are derived from the Architecture Overview and from direction by the Project:

Ref	Requirement	Action taken
R1	Support for virtual hosting infrastructure	Solution will host on a one-node running the Hyper-V hypervisor on Primergy servers (Customer choice). Second node could be added on later project stages to create Windows Failover Cluster. 1. Included in the license cost required for the windows servers 2. Hyper V will shutdown the virtual machines while patching of the physical host 3. Hyper V is supported as a virtualisation platform for all applications and services within the infrastructure
R2	Alerting for all components. The following items must be monitored: Windows VMs Hyper V servers	Azure Monitor will be used to monitor infrastructure
R3	Reduced cost	In order to ensure the lowest price point, one host Hyper-V deployed each site utilising failover at application level where possible while still maintaining desired RTO.
R4	Fujitsu RX2540 and TX2550 Servers	The Fujitsu RX2540 M5 server is a 2U 2 socket server that will minimise the data centre footprint while still providing the right mix of internal disk capacity, IO connectivity and CPU/Memory for the hypervisor. The TX2550 M5 server is tower model for locations without a rack solution present.
R5	Azure Update Management. Patching service for Windows products across all management servers	On site servers will download patches via the Internet. In-guest clusters will use cluster aware updating.
R6	Windows Server 2019 OS	Windows 2019 is the latest version of windows available and supported by all components in the solution.

Ref	Requirement	Action taken
R7	Centralised Management. Active Directory	The solution will use an domain controllers located at each in scope site. User and computer security groups will be created to manage access and group policies to enforce controls and compliance. Active directory sites will allow infrastructure components to authenticate services and users and apply security policies.
R8	Centralised Management. Virtualized environment	Windows Admin Center and Failover Cluster Manager are required to configure and manage the Hyper-V infrastructure WAC will be deployed on a single server running on Azure cloud
R9	Storage Spaces Capacity disks	The 4x HD SAS 12G 10K 512e HOT PL 2.5' EP (1.2, 1.8 or 2.4 TB based on server size type) will be used for the capacity tier, excluding the boot disks. RAID 5 will be used.
R10	OS disk mirrored onto 2 drives.	The 2x SSD SATA 6G Mixed-Use 2.5' H-P EP (240GB or 480GB based on server size type) will be used for OS boot disk.

Table 1 – Requirements Traceability

2.2.2 In Scope

This High Level Design covers the following areas:

- Infrastructure location, server hardware.
- Virtualisation configuration, management.
- Virtual machine templates and provisioning.
- Management server roles for; Active Directory, File, Print.
- Backup and Security integration – Firewall rules / AV exceptions.
- Resilience and disaster recovery.
- Support and Enterprise Management integration.
- Testing criteria.

2.2.3 Out of Scope

The following are excluded from the scope of this design:

- Design and configuration of storage and backup.
- Design and configuration of System Centre Operations Manager.
- Design and configuration of the payload application.
- Design and configuration of the network schema, IP and port allocations and firewalls.

2.3 Background

Barenbrug is globally second player in the domain of grass seed development and delivery. Goal is to sustain that position. For that Barenbrug needs to upgrade their IT environment and comes into control of IT spend. The factories are mission critical.

Barenbrug selected Fujitsu as single partner for all global IT. Fujitsu proposed blue print best practices for an end-to-end workplace services environment based on public cloud, Microsoft 365, SaaS and Fujitsu hardware.

Future mode of operation (FMO) will be cloud based: Azure cloud which is ready to adopt new technologies.

Greenfield approach has been selected. Fujitsu offered a solution that will ensure a standardized IT-environment for Barenbrug. In scope site solution will be based on Hyper-V and Fujitsu Primeflex servers.

In order to achieve these objectives:

1. Introduce latest generation technology into Barenbrug's data centres and businesses
2. The initial Design phase of Project activities will seek to allow for Azure requirements generated by other (transitional) Barenbrug projects, where these can be defined and do not significantly impact the time to complete or cost of design work
3. On next project phases migration activities will be managed in a flexible and agile manner, with changes (e.g. Transitions) of workloads accommodated up to an agreed cut-off date for each migration wave
4. Enable flexible utilisation-based charging across the services

2.4 Risks, Assumptions, Issues and Dependencies

2.4.1 Risks

Ref No	Risk	Probability	Impact	Action
R01	VPN connectivity is down between Barenbrug and Azure IaaS	L	M	A resilient VPN solution will be considered.
R02	Single Hyper-V host is a single point of failure	L	H	At future project stages add 2nd host for resilience.

2.4.2 Assumptions

Reference	Assumption
A1	The information contained with the AOD and RTM is a true and accurate reflection of the requirements.
A2	This HLD is a Define level document subject to amendment at future stages of the project lifecycle.
A3	New provisioned servers will use Windows Server 2019 as an operating system.
A4	Azure backup solution will be used to backup infrastructure and native Azure monitoring tools will be leveraged for this purpose.
A5	All the technical deployment details are based on the current Azure platform capabilities.

Table 2 – Assumptions

2.4.3 Issues & Unknowns

None at this point.

2.4.4 Dependencies

Reference	Dependency	Impact	Dependency On
D1	A shared management network design and implementation	The ability to manage the infrastructure	Fujitsu
D2	VPN from Azure region to location based on ISP of Barenbrug	The ability to manage the infrastructure	Fujitsu

Reference	Dependency	Impact	Dependency On
D3	Provision of power and space in datarooms within medium locations	The capability will not be able to installed in strategic locations	Barenbrug
D4	Initial hardware setup and configuration in datarooms within medium locations	The infrastructure will not be able to be managed remotely	Fujitsu
D5	Training of Design/operational support staff	The infrastructure will not be able to be managed	GDC Russia
D6	Provision of Internet links	The solution will not be able to provide internet backup/archive capability	Barenbrug
D7	TFSnow	To handle call routing	TFSnow service team

Table 3 – Dependencies

2.5 Constraints (Standards, Policies, Guidelines)

No.	Description
C1	All solutions and technologies deployed must be available and supportable at the time of design
C2	All designs will adhere to the Fujitsu IDBM process and governance
C3	Solution must be compliant with contractual storage and data management policies

Table 4 – Constraints

2.6 Impact on Existing Infrastructure

There is no impact on existing infrastructure as this is a new service being provisioned in the identified medium locations as a greenfield setup.

3. Design Overview

3.1 Overall Description

The key points of this solution are as follows:

- This greenfield solution will be hosted across locations in the following Barenbrug locations:
  - The Netherlands
  - France
  - United Kingdom
  - Luxemburg
  - United States of America
  - Brazil
  - Argentina
  - Australia
  - New Zealand
- Each site will have one Primergy server rack or tower mounted and cabled, by engineering services to Fujitsu standards, to diverse; power and network end points.
- Each site will have site to site VPN connection to one of Azure regions: West EU, West US, Australia Central.
- Each Primergy server will be running Microsoft Windows Server 2019 edition with the Hyper-V role and managed by Microsoft Windows Admin Center creating hosting platform for the infrastructure and application virtual machines although exceptions will be made based on compatibility.

- Storage for virtual machinve will be provided by storage spaces in the Hyper-V host.
- The solution will have 1 Read Only Domain Controller (RODC) in each selected location providing centralised and replicated:
    - Authentication for servers and infrastructure components.
    - Security controls and compliance via group membership and group policy.
    - Time source for synchronisation.
    - DNS.
- The solution will have 1 server hosting Bartender application.
- The solution will have Cisco Meraki backbone per site to manage and monitor the network infrastructure
- The solution will use Azure Monitor to provide enterprise management alerting and reporting. Alerts will be sent to TfsNow.
- Solution infrastructure management servers will only be backed up is there is changing data including using Azure Backup. All other components like RODC will be recovered by re-provisioning. See Ref2 for more info.

3.2 Design Diagram(s)

3.2.1 Physical Solution Overview

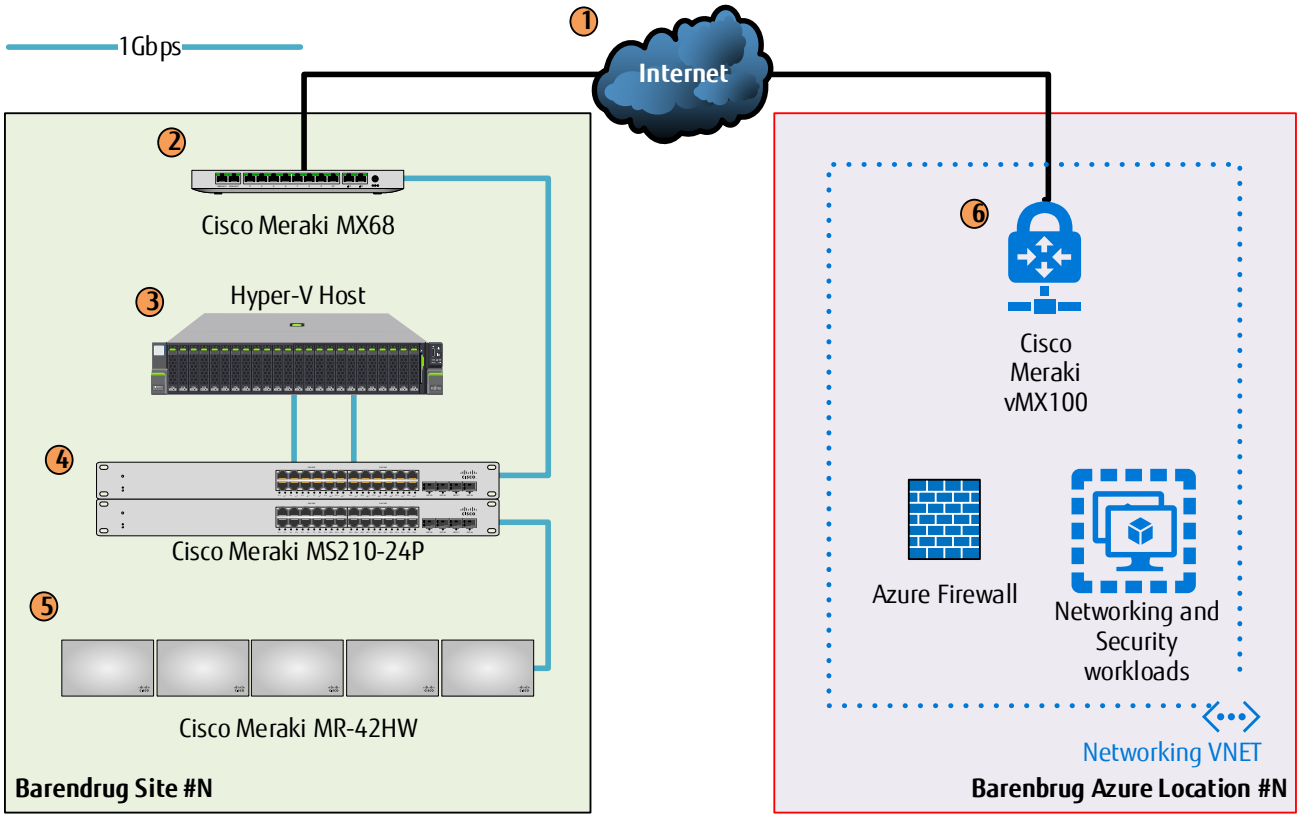

Figure 1 – Physical Solution Overview

Component No.	Description
1	Internet Connectivity: used by customers to consume the service and infrastructure components to connect to external services. For detailed design section please see Network HLD/LLD in References.
2	Cisco Meraki MX68: routing connectivity in and out of the data centres. For detailed design section please see Network HLD/LLD in References.
3	Hyper-V Host: Primergy server running Windows 2019 Data Center edition with Hyper-V, virtual machines, storage spaces, virtual network switch. Dual paths for network connectivity.
4	Cisco Meraki MS210-24P: providing layer 2/3 connectivity for all devices. For detailed design section please see Network HLD/LLD in References.
5	Cisco Meraki MR-42HW: indoor access points for all clients.
6	Cisco Miraki vMX100: virtual instance of a Meraki security & SD-WAN appliance, site-to-site VPN termination.

Table 5 – Solution Overview Component Description

3.2.2 Logical Solution Overview

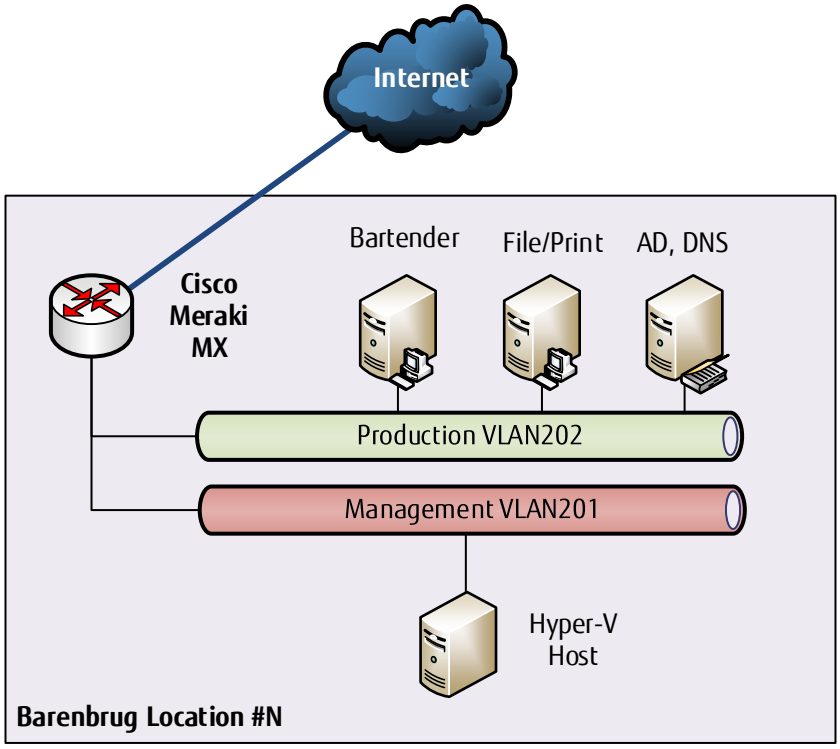

Figure 2 – Logical Solution Overview

3.2.3 Context Diagram

The diagram and table below provides a contextual overview of components and services, which the solution will integrate with.

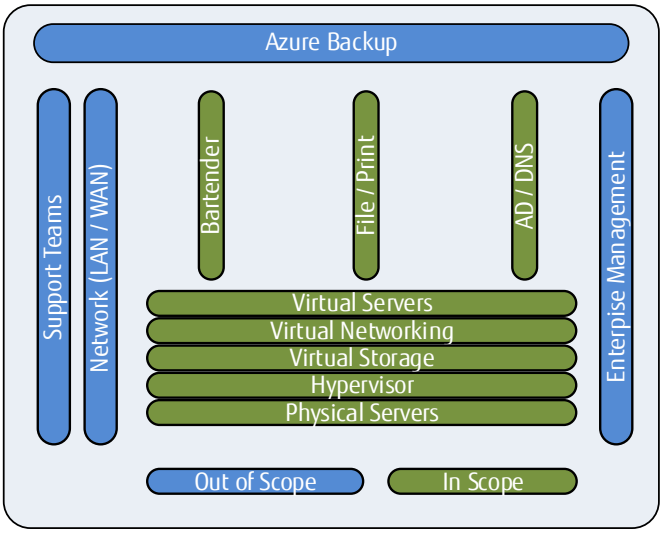

Figure 3 – Context Diagram

4. Addressing Functional Requirements and Design Decisions

4.1 Physical Locations

Country	Address
The Netherlands	Barenbrug Holland BV Stationsstraat 40 6515 AB Nijmegen Tel: +31 24 3488100 Email: info@barenbrug.nl
France	BARENBRUG France S.A. 14 avenue de l'Europe CS 60705 MONTEVRAIN 77772 MARNE LA VALLEE CEDEX 4 France
France	Barenbrug Connantre Chemin Sézanne 51230 Connantre Tel: 03 26 81 08 83
United Kingdom	Barenbrug UK 33 Perkins Road Rougham Industrial Estate Bury St Edmunds Suffolk IP30 9ND Tel: +44 (0) 1359 272000 Email: info@barenbrug.co.uk
Luxemburg	Barenbrug Luxemburg S.A. Zone Industrielle 55 L-9099 Ingeldorf +35 2 808484
United States of America	Barenbrug USA Corporate Office: 33477 Highway 99E PO Box 239 Tangent OR 97389 Phone: 800-547-4101
Argentina	Barenbrug Argentina Calle Álvarez Condarco 612 B2700 Pergamino Buenos Aires +54 9 2477 663461
Brazil	Commercieel: Av. Presidente Vargas 2121 Sala 1808 CE Times Square Ribeirao Preto SP Brazilië CEP 14020-260 +55 (16) 3325 6770
New Zealand	2547 Old West Coast Road RD 1 Christchurch 7671 Ph 03 318 8514 New Zealand

Country	Address
Australia	VICTORIA (HEAD OFFICE) 26 Prosperity Way (Off Jayco Drive) Dandenong South VIC 3175, Australia T: (03) 9701 4000 F: (03) 9701 4040

Table 6 – Physical Locations

The bill of materials (System Architect) can be found in **References**.

The rack layout of components can be found in the Port Allocation guide in **References**.

4.2 Naming Convention

The device naming convention for the project follows:

- [1-3] – Alpha Numeric - BRG: name of the project
- [4-8] – Alpha Numeric - Site: location of the device; FR01 or US01
- [9-11] - Alpha Numeric - Role: role of the server such as; ADR, HPV, FPS.
- [12-13] - Numeric - Increment: instance counter of each role,

Role Code	Role Description
BAR	Bartender
ADR	Active Directory Server, RODC
ADW	Active Directory Server, RWDC
HPV	Hyper-V Host
FPS	File Print server
WAC	Windows Admin Center server

Table 7 - Server Role Codes

4.3 Hyper-V Hosts

Design decisions

Decision	Rationale
PRIMERGY RX2540 and TX2550 M5 Servers	The Fujitsu PRIMERGY RX2540 M5 server is a 2U 2 CPU socket server that will minimise the data centre footprint while still providing the right mix of disk connectivity and CPU/Memory for the hypervisor. Additional tower model, PRIMERGY TX2550 M5 for locations without a rack solution present.
Hyper-V	The reason for implementing Microsoft Windows Server 2019 with the Hyper-V role is to support the virtual machine requirement for the Active Directory, Enterprise Management and other applications being deployed as part of the project with potential for future expansion to support other workloads.
2 x Intel Xeon Silver 4214 12C 2.20 GHz for Medium and Large Or 2 x Intel Xeon Silver 4208 8C 2.10 GHz for Small	The use of two Intel Xeon Silver Processors per server has been selected based on server size type (Small, Medium and Large). This CPUs was selected due to the high logical core count per socket.
256GB RAM for Large and made up of 8 x 32GB (1x32GB) 2Rx4 DDR4-2933 R ECC or	This level of RAM has been chosen because standard Server memory is 64GB and it was doubled for future needs to ensure adequate resource access and limit RAM contention as RAM is the number one constraint in Virtualised environments for Medium and Large server types. It is more then enough for greenfield approach and if we will

Decision	Rationale
128GB RAM for Medium and made up of 4 x 32GB (1x32GB) 2Rx4 DDR4-2933 R ECC Or 64GB RAM for Small made up of 2 x 32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	assume that 12GB RAM will be used by each VM we will be able to run 20VMs on the Hyper-V cluster in case of server memory is mapped on a 1:1 basis.
2x SSD SATA 6G 480GB Mixed-Use 2.5' H-P EP for Medium and Large Or 2x SSD SATA 6G 240GB Mixed-Use 2.5' H-P EP for Small	The SSD SATA 6G will be used for OS boot disk with capacity based on server size type.
4x HD SAS 12G 2.4TB 10K 512e HOT PL 2.5' EP for Large 4x HD SAS 12G 1.8TB 10K 512e HOT PL 2.5' EP for Medium 4x HD SAS 12G 1.2TB 10K 512e HOT PL 2.5' EP For Small	The HD SAS will be used for the stroge spaces direct capacity tier, excluding the boot and cache disks. The RX2540M5 can hold maximim 20 server size type capacity disks.
An integrated Remote Management Controller.	Each server will be equipped with an iRMC adapter providing full remote server functionality in case of an operating system failure using SNMP traps to send failure notifications to System Center Operations Manager toolset, the adapter will have an integrated network interface to avoid any incompatibility with the payload interface team.
Support	The servers will receive firmware patches from the update manager component in Fujitsu ServerView which covers all supported hardware components controlled by change management and initiated by support teams.
Support	Hardware component failures are supported by a Fujitsu Engineering services contract covering 3 years providing a 4 hour response 24x7.
As the solutions expands additional Hyper-V hosts can be added to increase available resources	To meet future growth of the solution, there is sufficient rack space in the data centre and network and storage capacity to install additional physical servers.

Table 8 – Hyper-V hosts design decisions

The bill of materials can be found in Error! Reference source not found. and System Architect configuration in **References**.

4.4 Microsoft Windows 2019 Server Hyper-V

Design decisions

Decision	Rationale
Deployment of Hyper-V role on Windows Server 2019 Datacenter.	To increase utilisation of the hardware that will be used for the infrastructure, as well as reducing the initial footprint, a hypervisor will be used to virtualise the management servers and application servers. Both VMware and Hyper V are supported by Fujitsu, Hyper V will be selected for the following reasons:- 1. Included in the license cost required for the windows servers 2. Hyper V supports migrating the virtual machines online allowing for patching of the physical host 3. Hyper V is supported as a virtualisation platform for all applications and services within the infrastructure Storage spaces will be used for virtual machine storage as this is included in the windows license. Windows Server 2019 is the latest version of windows available and supported by all components in the solution. As such will be the operating system deployed to all windows servers.
Network connectivity provided by Switch Embedded Teaming (SET) team with RDMA-capable physical NICs.	SET is an alternative NIC Teaming solution that you can use in environments that include Hyper-V and the Software Defined Networking (SDN) stack in Windows Server 2019. SET integrates some NIC Teaming functionality into the Hyper-V Virtual Switch. SET allows you to group between one and eight physical Ethernet network adapters into one or more software-based virtual network adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure. Next cards will be installed: 1x PLAN CP 4x1Gbit Cu Intel I350-T4 – small, medium tower servers 1x PLAN EM 4x 1Gb T OCP interface – small, medium rack servers 1x PLAN EM 2x 10Gb T OCP interface – large rack servers
Azure Update Management will be used.	Although SCCM could patch the environment it seems overly complex for the environment. As such a Azure Update Management will be used for patching the infrastructure.
Microsoft Defender to provide server threat and enpoint detection.	Microsoft Defender extends support to also include the Windows Server operating system.
Azure Monitor to be used for monitoring and integrated with Check_MK, Check_MK will manage support tickets into TfsNow.	As the Azure Monitor is licensed for the use of Hyper-V solution. All components such as the hardware and software of solution are covered.
Receive NTP services from the Active Directory.	Time will be synchronised from the Active Directory servers (stratum 3).
Access and support	Access to the virtual servers will be managed and audited using Active Directory security groups and group policies. Management of the servers will be done using RDP or management GUIs from the jump server.
Backup and Recovery	Hyper-V hosts will not be backed up, instead the host will be rebuilt due to the simple configuration giving downtime for VMs running on it during recover period (see Risk R02).

Table 9 - Windows 2019 Server Hyper-V design decisions

4.4.1 Virtual Networking

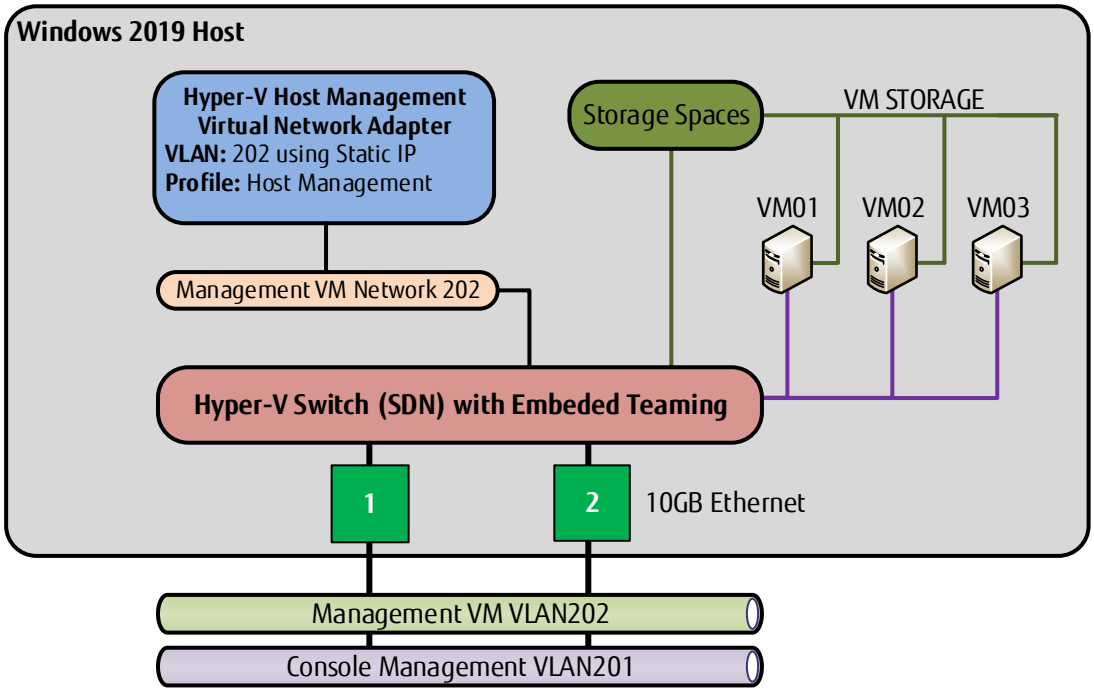

Figure 4 – Virtual Networking

Each Hyper-V host will have the 2 x 10GB or 4 x 1GB interfaces. On the first virtual layer there will be deployed SET switch that include Hyper-V and the Software Defined Networking (SDN) stack. SET integrates some NIC Teaming functionality into the Hyper-V Virtual Switch. SET allows to group physical Ethernet network adapters into one or more software-based virtual network adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure. On the second virtual layer there will be defined virtual network adapter: Management. It will be configured with a proper port profile classification and VLAN to facilitate Hyper-V function.

The network components will be monitored by Azure Monitor and the network switches managed by the NOC and monitored by Check_MK. The 2 port load balanced interfaces and use of virtual networks in Hyper-V provide sufficient capacity for future growth with scale out options by adding additional servers.

4.4.2 Storage Spaces

Storage Spaces is a technology in Windows and Windows Server that can help protect your data from drive failures. It is conceptually similar to RAID, implemented in software. You can use Storage Spaces to group three or more drives together into a storage pool and then use capacity from that pool to create Storage Spaces. These typically store extra copies of your data so if one of your drives fails, you still have an intact copy of your data. If you run low on capacity, just add more drives to the storage pool.

Leveraging the 4x 2.5" high-capacity drives such as HD SAS HDDs that will be used in this solution, each server is itself a JBOD (just a bunch of disks) repository.

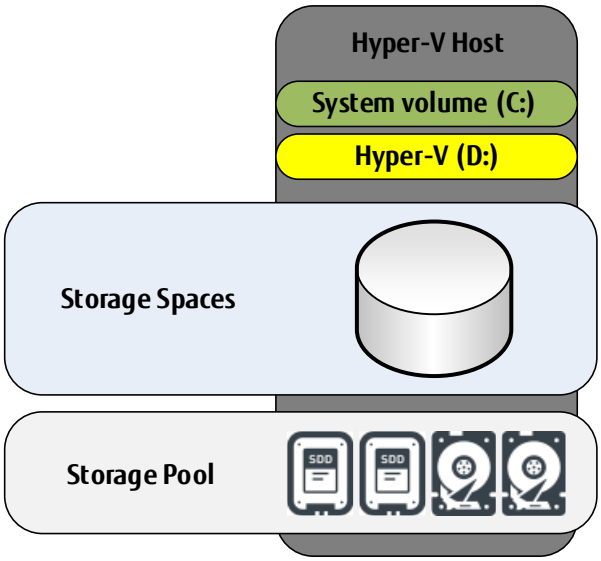

Figure 5 - Virtual Storage

Faster-performing SSD devices (SSD SATA 6G 240GB or 480GB Mixed-Use 2.5' H-P EP) will act as a OS drive with SWAP. Data is mirrored across 2 drives, thus allowing for very fast retrieval from multiple read points.

Traditional disk subsystem protection relies on RAID storage controllers. In Storage Spaces, high availability of the data is achieved using a non-RAID adapter and adopting redundancy measures provided by Windows Server 2019 itself. The storage can be configured as simple spaces, mirror spaces, or parity spaces.

Mirror spaces: Stripes and mirrors data across a set of pool disks, supporting a two-way or three-way mirror, which are respectively resilient to single disk, or double disk failures. Suitable for the majority of workloads, in both clustered and non-clustered deployments. In this solution three-way mirror will be used.

4.5 Hyper-V Virtual Machine

Virtual machines will be provisioned using the WAC console for the appropriate Hyper-V host, the VM will be placed on to Storage Spaces.

Microsoft Windows Server 2019 will be used for all VMs deployed in the solution. The Windows server license will be activated by the use of the Hyper-V server Datacenter edition with no limitations on VMs count. All servers will be joined to the domain.

Access to the virtual servers will be managed and audited using Active Directory security groups and group policies. Each host will be monitored using Azure Monitor which will send alerts on resources and application thresholds. Threat prevention will be managed by Windows Defenter and controlled through policies which can apply exclusions based on the server role.

Virtual machine profiles can be found in the Ref2.

4.6 Windows Admin Center

Windows Admin Center (WAC) has been chosen to manage and monitoring the Hyper-V resources, a single instance of WAC will be deployed in Azure West EU region in a jumpbox. It could be deployed on central office terminal server as well in the future. Jumpboxes could be clustered in the future based on the load.

Windows Admin Center is the next-generation management tool for Windows Server, the successor to traditional "in-box" tools like Server Manager. It's free and can be installed and used without an Internet connection. You can use Windows Admin Center to manage and monitor Hyper-Converged Infrastructure running Windows Server 2016 or Windows Server 2019.

WAC provides a role based access model to controls Hyper-V configuration and can be restricted using Active Directory security groups. However, this is only available when installing WAC in gateway mode on a Windows Server.

Traffic from the browser to the Windows Admin Center gateway uses HTTPS. Traffic from the gateway to managed servers is standard PowerShell and WMI over WinRM. It supports LAPS (Local Administrator Password Solution), resource-based constrained delegation, gateway access control using AD or Azure AD, and role-based access control for managing target servers.

Windows Admin Center can be installed on Windows 10 Fall Anniversary Update (1709) or newer, or Windows Server 2016 or newer. To manage Windows Server 2008 R2, 2012, or 2012 R2, installation of Windows Management Framework 5.1 is required on those servers. There are no other dependencies. IIS is not required, agents are not required, SQL Server is not required.

WAC will help to integrate Hyper-V hosts with Azure Monitor to enable alerting and reporting of hypervisor hosts and virtual machines, availability and resilience is underpinned by the Hyper-V platform. Backup of the WAC is not considered as it could be reinstalled from the scratch any time using msi installation source file.

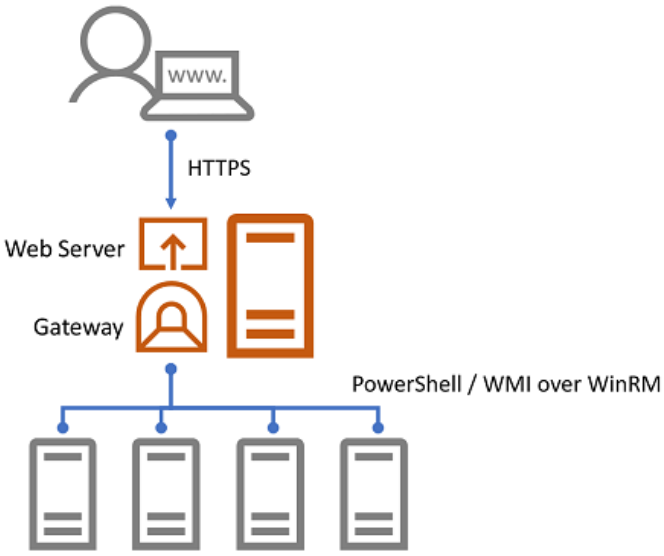

Figure 6 - WAC Architecture

4.6.1 Networking

WAC will be used to deploy a single management SET switch using an switch independent profile for load balancing the physical interfaces on the host, port profiles will be implemented to ensure the correct bandwidth is allocated based on the network function; medium bandwidth profile is the default for VMs to ensure balanced throughput, host cluster workload for the Hyper-V inter-host communication, live migration workload for transfer of VMs between hosts and host management.

Using the logical switch, a logical network will be created with a definition for its local site including site name and VLANs with their IP networks. Within the logical switch, IP pools will be created for each logical network offering either automatic or static IP allocation to VMs.

Finally, virtual networks will be created for each VLAN binding together the; logical switch and IP pools. Hyper-V hosts are configured with a single interface on the management network so they can be discovered by WAC at which point the management switch is deployed to the host so it can join the cluster.

4.6.2 Library for VM template

Windows Server 2019 template will be used, the template will be built of Windows Server 2019 and stored in the same place as running VMs. The template will be used to provision new virtual machines and join them to the domain using a guest OS profile, this process has a dependency on a dedicated AD account that has domain user privileges being registered in WAC.

4.6.3 Virtual Machines

VMs will be deployed using WAC based on the VM template in the library. Storage will be allocated from the storage pool for the desired tier of storage, disks will be dynamic and stored using the VM hostname and function of the disk (e.g. ServerA_OS.vmdk, ServerA_Data.vmdk). Network interfaces will be allocated based on the required VLAN in the solution with the correct bandwidth profile applied based on the role (server role, cluster role).

Memory will be statically allocated in Hyper-V as the solution has been sized to operate at full capacity. This option has also been considered based on the lessons learnt from deployment where applications would not function correctly when dynamic memory allocation was selected.

The solution has multiple VMs participating in the same functional role so having them running on the same physical host could result in an outage should that host experience failure whether it's: patching, hardware or software, connectivity or user error. Affinity and antiaffinity rules will be created for each functional role preventing them from being resident on the same physical host.

4.7 Azure Monitor

Azure Monitor will monitor components in each Hyper-V site. IT Service Management Connector (ITSMC) for Azure (ITSMC) provides bi-directional integration between Azure monitoring tools and ITSM tool – TfsNow. But in this case it will be integrated with Check_MK with further integration with TfsNow for incidents management. Integration part is out of current document scope.

Azure Monitor collects, analyzes, and acts on telemetry from a variety of resources, including Windows servers and virtual machines (VMs), both on-premises and in the cloud. Though Azure Monitor pulls data from Azure VMs and other Azure resources, this section focuses on how Azure Monitor works with on-premises servers and VMs running on Hyper-V, specifically with Windows Admin Center.

4.7.1 Azure Monitor workflow

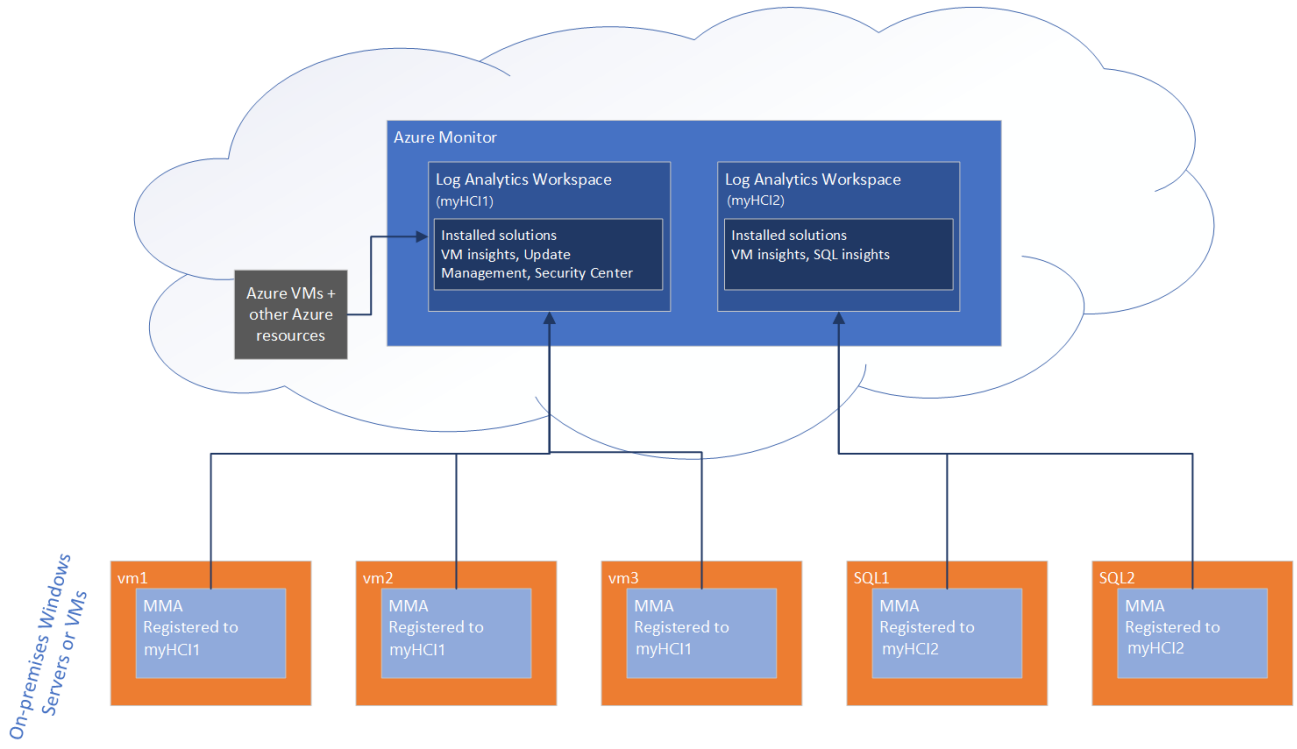

Figure 7 - Azure Monitor workflow

Data generated from on-premises Windows Servers is collected in a Log Analytics workspace in Azure Monitor. Within a workspace, you can enable various monitoring solutions–sets of logic that provide insights for a particular scenario. For example, Azure Update Management, Azure Security Center, and Azure Monitor for VMs are all monitoring solutions that can be enabled within a workspace.

When you enable a monitoring solution in a Log Analytics workspace, all the servers reporting to that workspace will start collecting data relevant to that solution, so that the solution can generate insights for all the servers in the workspace.

To collect telemetry data on an on-premises server and push it to the Log Analytics workspace, Azure Monitor requires the installation of the Microsoft Monitoring Agent (MMA). Certain monitoring solutions also require a secondary agent. For example, Azure Monitor for VMs also depends on a ServiceMap agent for additional functionality that this solution provides.

Some solutions, like Azure Update Management, also depend on Azure Automation, which enables you to centrally manage resources across Azure and non-Azure environments. For example, Azure Update Management uses Azure Automation to schedule and orchestrate installation of updates across machines in your environment, centrally, from the Azure portal.

4.7.1.1 Data collected by Azure Monitor

All data collected by Azure Monitor fits into one of two fundamental types: metrics and logs.

Metrics are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. You'll see data collected by Azure Monitor right in the **Overview** page in the Azure portal.

Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis. Log data collected by Azure Monitor can be analyzed with queries to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using Log Analytics in the Azure portal and then either directly analyze the data using these tools or save queries for use with visualizations or alert rules.

4.7.1.2 Windows Admin Center and Azure Monitor

From within Windows Admin Center, you can enable three monitoring solutions:

- Azure Monitor for Clusters
- Azure Update Management (in the **Updates** tool)
- Azure Monitor for VMs (in server Settings), a.k.a Virtual Machine insights

You can get started using Azure Monitor from any of these tools. If you've never used Azure Monitor before, Windows Admin Center will automatically provision a Log Analytics workspace (and Azure Automation account, if needed), and install and configure the MMA on the target server. It will then install the corresponding solution into the workspace.

For instance, if you first go to the **Updates** tool to setup Azure Update Management, Windows Admin Center will:

1. Install the MMA on the machine.
2. Create the Log Analytics workspace and the Azure Automation account (because an Azure Automation account is necessary in this case).
3. Install the Update Management solution in the newly created workspace.

If you want to add another monitoring solution from within Windows Admin Center on the same server, Windows Admin Center will simply install that solution into the existing workspace to which that server is connected. Windows Admin Center will additionally install any other necessary agents.

If you connect to a different server, but have already setup a Log Analytics workspace (either through Windows Admin Center or manually in the Azure Portal), you can also install the MMA on the server and connect it up to an existing workspace. When you connect a server into a workspace, it automatically starts collecting data and reporting to solutions installed in that workspace.

4.7.1.3 Azure Monitor for virtual machines

When you set up Azure Monitor for VMs in Server Settings, Windows Admin Center enables the Azure Monitor for VMs solution, also known as Virtual Machine insights. This solution allows you to monitor server health and events, create email alerts, get a consolidated view of server performance across your environment, and visualize apps, systems, and services connected to a given server.

Despite its name, Virtual Machine insights works for physical servers as well as virtual machines.

With Azure Monitor's free 5 GB of data/month/customer allowance, you can easily try this out for a server or two without worry of getting charged. Read on to see additional benefits of onboarding servers into Azure Monitor, such as getting a consolidated view of systems performance across the servers in your environment.

5. Non-Functional Requirements

The following sections show how the non-functional requirements are met by the design.

5.1 Availability & Resilience

5.1.1 Hyper-V Host Availability

Hyper-V host will be configured as a standalone host. This is Customer decision and all connected risks have been accepted by the Customer. If node fails, VMs will have downtime till node restoration. It is highly recommended to add second Hyper-V node and create a failover cluster for high availability. See Infrastructure applications HLD/LLD Ref2.

5.1.2 WAC Availability

The WAC will be installed on the Terminal server in Azure. It should be noted that in the unlikely event of the WAC becoming unavailable due to mis-configuration or corruption, virtual infrastructure operations will continue to function and WAC will be rebuild from the scratch (see section 4.6).

5.1.3 Resilience

Single PRIMERGY RX2540 M5 server will have resilient components including redundant power supplies (PSU); teamed network cards (NIC), redundant host bus adaptors (HBA) and RAID configured hard disk drives. The integrated Remote Management Controller (iRMC) will be configured to allow for out of band connectivity. The iRMC provides capability to allow for remote access to the server for shutdown, start-up and other management capabilities even when the server is not accessible via connected standard networks. The iRMC will be configured following standard PRIMERGY documentation.

The following diagram displays connection resilience at a logical level:

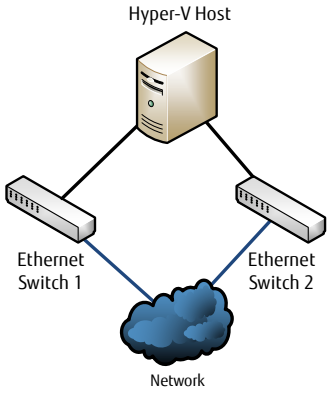

Figure 8 – Host Multipathing

5.2 ICT Continuity

There is no defined Recovery Time Objective (RTO) or Recovery Point Objective (RPO). Disaster recovery services will be provided on application layer where it is possible. Applications leveraging these disaster recovery tools may require their own additional recovery steps to provide seamless failover to the end user; these steps will be detailed in individual subsystem low level designs.

5.3 Capacity and Performance management

Performance and capacity will be monitored via Azure Monitor - statistical information will be captured ready for report generation.

The virtual environment by manufactures design is able to grow on a component by component basis. Additional memory and interface hardware can be added to the PRIMERGY RX2540 M5 rack server to provide further capacity. Expansion of the disks can be performed to provide more storage to the virtual machines hosted on the Hyper-V server. All virtual environments have been sized to include growth as per customer information.

5.4 Security

Fujitsu's approach will be to utilise formally assured products where available for all areas of security enforcing functionality. This design specifically will address security vulnerabilities in the virtual infrastructure. The following measures will be deployed:

- Windows Firewall will be enabled on all Hyper-V hosts.
- VMs will only connect to virtual switches belonging to the same security domain.
- Role based access control to all virtual infrastructure components.
- Authentication will be provided by Active Directory Services securely deployed inside the virtual environment.
- Day to day operational compliance against ISO27001.

Firewall access control rule sets will need additions/amendments to satisfy traffic flow requirements of the virtual environment. Patching and remote management functionality will require firewall configuration. Ports, traffic flow and routing information will be provided in the virtual infrastructure low level design in conjunction with the network architect.

5.5 Other Service Levels

Barenbrug infrastructure and associated service levels not covered by this design.

5.6 Supportability

Support and management of the virtual infrastructure will be the responsibility of the GDC RU RIM WINTEL capability unit which will use an established means of remote connectivity via the Fujitsu Global WAN infrastructure. From the Global WAN infrastructure Fujitsu have dual MPLS in place to both of the Vodafone data centres in the UK. The MPLS both have diverse routing in place for further redundancy.

The Barenbrug Remote Desktop Services server will provide management tools to enable remote administration of the implemented infrastructure. These tools will include, WAC, Remote Server Administration Tools and Hyper-V Console.

5.6.1 Support Teams

Component	Support Unit
Hyper-V Hosts, Admin TS, WAC Server, Virtual Machines Ongoing Support	Support of the hosts and Hyper-V will be the responsibility of RIM Wintel, which delivers a blended model solution to Barenbrug. This blended model is delivered from GDC RU RIM WINTEL.
Microsoft 4th Line Support	PTSG
PRIMERGY server HW	Fujitsu

Table 10 – Support Teams

5.6.2 Support Training Requirements

The following courses would prove beneficial for virtualisation support staff "Implementing and Managing Microsoft Server Virtualization" course code: 10215 and "Server Virtualization with Windows Server Hyper-V and System Center" course code: 20409.

5.6.3 Backups

Backup of the implemented infrastructure will be provided by a newly provisioned backup environment based on Microsoft Azure Backup (MAB). The platform should be enabled to accommodate virtual machine backup rather than use a conventional agent based backup as it is more efficient and flexible.

Each of the Hyper-V hosts will require backup due to the complex nature of configuration. An agent should be deployed to each host to facilitate this. A number of backup exclusions are required for the Hyper-V hosts; more detail will be provided in the LLD.

The WAC server should be backed up utilising a virtual machine based back up, if this is not possible then an agent should be installed to accommodate for the backup requirement.

All of the components within this design will require at least a weekly full, daily incremental and monthly full backup. More detail will be available in the LLD.

5.6.4 Anti-Virus

Anti-Virus protection of the implemented infrastructure will be provided by a Microsoft Defender build in application. All Hyper-V hosts and virtual servers will be protected by the Microsoft Defender. A number of anti-virus exclusions are required for the Hyper-V hosts; more detail will be provided in the LLD.

5.6.5 Supporting Contracts

Use of Fujitsu's Microsoft Premier Support Agreement will be leveraged for the Microsoft based virtualisation tools. Service hours provided by these go over and above what is required by the Barenbrug contract. Fujitsu will be able to maximise the benefit of these extended hours when supported problem resolution is required out of hours to ensure availability metrics are not breached.

5.7 Enterprise Management

Management of the virtual environment will be utilising the following toolsets:

- **Azure Monitor** will provide monitoring for the PRIMERGY servers.
- **Windows Admin Center** will provide a holistic management view of the virtual infrastructure; it will allow configuration of custom alerts and integration of logging capabilities. Logs and alerts will be passed to the Azure Monitor via management packs.
- **Microsoft Remote Desktop Services** will provide an administration point for all virtual components.
- **Fujitsu iRMC** will allow a remote management function for all hosts.

More information regarding enterprise management can be found in the Barenbrug Azure Infrastructure and Check_MK HLDs and LLDs.

5.7.1 Remote Support

Please see section 5.6 for more information.

5.8 Interoperability & Integration

The main interoperability points for the virtualisation components are network devices. Integration into the Azure Monitor enterprise management service will also be a key point.

5.9 Compatibility

This solution is compatible with the Barenbrug infrastructure and will act as a core component of it. The solution proposed for Barenbrug will also provide easy scale out and up capability should it be required in the future. To scale out the capacity of the future Hyper-V cluster more servers can be added up to the 64 node limit of the cluster.

6. Implementation and Deployment

6.1 Implementation Order

6.1.1 PRIMERGY RX2540 M5 Rack Servers / TX2550 M5 Tower Servers

Servers will be racked and connected to power, network and VDU resources. BIOS and firmware upgrades of all server components should be initiated at this stage. The iRMC interface addressing information will be configured at this stage also.

6.1.2 IP Addressing

All IP addresses will be agreed with Barenbrug. A list of required IPs will be drawn up at the LLD stage and requested. See Network HLD/LLD Ref3 for more info.

6.1.3 Hyper-V Hosts

Hosts will be provisioned using the iRMC interface. ISO files containing the Windows Server operating system will be attached to the iRMC console and installation will begin. Once installation is complete the relevant network teams will be configured and Management IP addressing and DNS information will be added. Then the appropriate roles installed onto the OS, Hyper-V. Build information will be available in the LLD. A server 2019 build image will be made available by the project and stored in ISO format on the Hyper-V Server.

6.1.4 WAC Server

A routable connection to the first Hyper-V Windows Operating system via RDP will allow the creation of the WAC server. Configuration of the server operating systems will follow the standard creation process.

6.1.5 Virtual Machines

Due to network bandwidth constraints the ISO library will need to be locally uploaded to the Hyper-V server. A virtual machine with the Windows Server 2019 Fujitsu exemplar build will be provisioned into templates. Subsequent Windows 2019 Server virtual machines will be deployed from these respective templates.

6.2 Methods of Deployment

Predicted change to Barenbrug virtual infrastructure is low. Manual installation using iRMC interfaces has been chosen.

6.3 Resources and Skill Sets

- PRIMERGY RX2540 M5 Server Installation, Configuration and Operation
- PRIMERGY TX2550 M5 Server Installation, Configuration and Operation
- Microsoft Windows Server 2019 Installation, Configuration and Operation
- Microsoft Hyper-V 2019 Installation, Configuration and Operation
- Microsoft Admin Center Installation, Configuration and Operation

7. Migration

A migration of all virtual machines is not required in this project stage.

8. Testing and Acceptance Strategy

8.1 Hardware Testing

Hardware and server build testing will be completed in factory prior to shipping.

All systems will be functionally tested during the implementation phase.

8.2 Resilience Testing

Resilience testing should take place to determine that all components and configurations that contribute to the resilience of the solution perform as designed and that the solution can withstand failure of those components. This testing should consider physical components such as dual power supplies or dual connections to network switch or indeed complete servers.

Physical server tests:

- Test failure to one of the host server PSU by disconnection
- Test failure to one of the NIC connections by disconnection

Virtualisation Hosts:

- Recovery of a Hyper-V host from total failure

Network:

- Test LAN resilience by powering off switch

8.3 Enterprise Management Testing

Failover events will be reproduced to ensure alerts are raised to the appropriate team. Remote access methods will be tested to ensure management activities can take place during production.

8.4 Disaster Recovery Testing

DR tests are not planned.

8.5 Usability Testing

Usability of the virtual platform will be tested using the following tests:

- Virtual Machine deployment from template
- Virtual machine creation
- Virtual power and reboot functions
- Adding and removing virtual hardware from virtual machines

8.6 Acceptance into Service

Acceptance into service will need to be granted by operational teams once hardware, resilience, enterprise management, disaster recover and usability testing is complete.

9. Low Level Design Approach

One virtual infrastructure LLD for Barenbrug will require creation; Microsoft Windows Server 2019 with the Hyper-V role. To achieve the final solution; it will contain the following functional descriptions:

- Hosts build and deployment
- Virtual switch configuration
- Virtual storage configuration
- Management server installation and configuration
- Licensing
- Virtual machine deployment
- Backup and Anti-Virus exclusions
- Integrating of virtual infrastructure into Azure Monitor
- Security hardening virtual infrastructure
- Network and Firewall configuration
- Testing
- Operational support
    - Remote admin tools

10. Bill of Materials

The following hardware is required to deliver this high level design. Other items relating to software, labour etc will be defined in additional project documentation and available in the project Share Point site:

Barenbrug Hyper-V S_M_L 23OCT2020 - optimized

10.1 Server Hardware

Common info: Rack based server 19" (2U) **and tower based server**, BU without processor and RAM, without hot plug power supply module, 3x2 hot plug fans redundant; RMK optional; dual systemboard for Xeon DP processor and 24 slots for registered DDR4 ECC RAM; iRMC S5 onboard server management incl. graphics controller and 10/100/1000MBit Service LAN port, LAN on Motherboard with 2x1Gbit/s (RJ45) plus the high performance Chip Intel LBG4 with flexble LAN connections - options for 4x1Gbit/s (RJ45), 2x10Gbit/s (RJ45), 2x10Gbit/s (SFP+) and 4x10Gbit/s (SFP+), Modular 8/16-Port RAID Controller optional; 24 drive bays for hot plug 2.5" SAS/SATA drives connected via SAS-expander; ServerView Suite Software Pack option.
Standard warranty:
3 years On-Site Service FTS wide / FTS 5 days / 9 hours (9x5, local business hours)

- X x PY RX2540 M5 8x 2.5' (**Large Rack**)

Product no.	Name	Quantity
S26361-F3776-E121	ErP Lot9 configuration for 1 DIMM	1
S26361-F4082-E114	Intel Xeon Silver 4214 12C 2.20 GHz	2
S26361-F3849-E100	Cooler Kit 2nd CPU	1
S26361-F3694-E10	Independent Mode Installation	2
S26361-F4083-E332	32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	8
S26361-F3718-E2	DVD ROM Ulltraslim	1
S26361-F5733-E480	SSD SATA 6G 480GB Mixed-Use 2.5' H-P EP	2
S26361-F5543-E124	HD SAS 12G 2.4TB 10K 512e HOT PL 2.5' EP	4
S26361-F5243-E11	PRAID EP400i	1
S26361-F5243-E155	FBU option for PRAID EP4xx	1
S26361-F5243-E100	TFM module for FBU on PRAID EP400i	1
S26361-F3953-E210	PLAN EM 2x 10Gb T OCP interface	1
S26361-F2735-E175	Rack Mount Kit F1 CMA QRL LV	1
S26361-F4530-E10	Mounting of RMK in symmetrical racks	1
S26361-F1452-E140	Region-kit Europe	1
S26361-F1790-E311	eLCM Activation License	1
S26361-F1790-E243	iRMC advanced pack	1
S26361-F2036-E100	ServerView Suite DVDs	1
S26113-F574-E13	Modular PSU 800W platinum hp	2
T26139-Y1968-E100	Cable powercord rack, 4m, black	2
S26361-F3552-E100	TPM 2.0 Module	1
S26361-F2567-E610	WINSVR 2019 DC 16Core OEM	1
S26361-F2567-E614	WINSVR 2019 DC AddLic 2Core OEM POS	4
FSP:GP3S60Z00NLSV2	TP 3y OS,9x5,4h Rt	1

Table 11 – PY RX2540 M5 8x 2.5' (Large Rack)

- X x PY RX2540 M5 8x 2.5' (**Medium Rack**)

Product no.	Name	Quantity
S26361-F3776-E121	ErP Lot9 configuration for 1 DIMM	1
S26361-F4082-E108	Intel Xeon Silver 4208 8C 2.10 GHz	2
S26361-F3849-E100	Cooler Kit 2nd CPU	1
S26361-F3694-E10	Independent Mode Installation	2
S26361-F4083-E332	32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	4
S26361-F3718-E2	DVD ROM Ulltraslim	1
S26361-F5733-E480	SSD SATA 6G 480GB Mixed-Use 2.5' H-P EP	2
S26361-F5730-E118	HD SAS 12G 1.8TB 10K 512e HOT PL 2.5' EP	4
S26361-F5243-E11	PRAID EP400i	1
S26361-F5243-E155	FBU option for PRAID EP4xx	1
S26361-F5243-E100	TFM module for FBU on PRAID EP400i	1
S26361-F3953-E401	PLAN EM 4x 1Gb T OCP interface	1
S26361-F2735-E175	Rack Mount Kit F1 CMA QRL LV	1
S26361-F4530-E10	Mounting of RMK in symmetrical racks	1
S26361-F1452-E140	Region-kit Europe	1
S26361-F1790-E311	eLCM Activation License	1
S26361-F1790-E243	iRMC advanced pack	1
S26361-F2036-E100	ServerView Suite DVDs	1
S26113-F575-E13	Modular PSU 450W platinum hp	2
T26139-Y1968-E100	Cable powercord rack, 4m, black	2
S26361-F3552-E100	TPM 2.0 Module	1
S26361-F2567-E610	WINSVR 2019 DC 16Core OEM	1
FSP:GP3S60Z00NLSV2	TP 3y OS,9x5,4h Rt	1

Table 12 – PY RX2540 M5 8x 2.5' (Medium Rack)

- X x PY RX2540 M5 8x 2.5' (**Small Rack**)

Product no.	Name	Quantity
S26361-F3776-E121	ErP Lot9 configuration for 1 DIMM	1
S26361-F4082-E108	Intel Xeon Silver 4208 8C 2.10 GHz	2
S26361-F3849-E100	Cooler Kit 2nd CPU	1
S26361-F3694-E10	Independent Mode Installation	2
S26361-F4083-E332	32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	2
S26361-F3718-E2	DVD ROM Ulltraslim	1
S26361-F5733-E240	SSD SATA 6G 240GB Mixed-Use 2.5' H-P EP	2
S26361-F5730-E112	HD SAS 12G 1.2TB 10K 512e HOT PL 2.5' EP	4
S26361-F5243-E11	PRAID EP400i	1
S26361-F5243-E155	FBU option for PRAID EP4xx	1
S26361-F5243-E100	TFM module for FBU on PRAID EP400i	1
S26361-F3953-E401	PLAN EM 4x 1Gb T OCP interface	1
S26361-F2735-E175	Rack Mount Kit F1 CMA QRL LV	1
S26361-F4530-E10	Mounting of RMK in symmetrical racks	1
S26361-F1452-E140	Region-kit Europe	1
S26361-F1790-E311	eLCM Activation License	1
S26361-F1790-E243	iRMC advanced pack	1
S26361-F2036-E100	ServerView Suite DVDs	1
S26113-F575-E13	Modular PSU 450W platinum hp	2
T26139-Y1968-E100	Cable powercord rack, 4m, black	2
S26361-F3552-E100	TPM 2.0 Module	1
S26361-F2567-E610	WINSVR 2019 DC 16Core OEM	1

Table 13 – PY RX2540 M5 8x 2.5' (Small Rack)

- X x PY TX2550 M5 Tower 8x2.5' (**Medium Tower**)

Product no.	Name	Quantity
S26361-F3776-E121	ErP Lot9 configuration for 1 DIMM	1
S26361-F4082-E108	Intel Xeon Silver 4208 8C 2.10 GHz	2
S26361-F3849-E100	Cooler Kit 2nd CPU	1
S26361-F3694-E10	Independent Mode Installation	2
S26361-F4083-E332	32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	4
S26361-F3266-E2	DVD-ROM 1.6" SATA	1
S26361-F5733-E480	SSD SATA 6G 480GB Mixed-Use 2.5' H-P EP	2
S26361-F5730-E118	HD SAS 12G 1.8TB 10K 512e HOT PL 2.5' EP	4
S26361-F5243-E11	PRAID EP400i	1
S26361-F5243-E155	FBU option for PRAID EP4xx	1
S26361-F5243-E100	TFM module for FBU on PRAID EP400i	1
S26361-F3953-E100	PLAN EM Blind Panel OCP	1
S26361-F4610-E4	PLAN CP 4x1Gbit Cu Intel I350-T4	1
S26361-F1452-E140	Region-kit Europe	1
S26361-F1790-E311	eLCM Activation License	1
S26361-F1790-E243	iRMC advanced pack	1
S26361-F2036-E100	ServerView Suite DVDs	1
S26113-F575-E13	Modular PSU 450W platinum hp	2
T26139-Y1740-E10	Cable powercord (D,..), 1.8m, grey	2
S26361-F3699-E20	Redundant power supply	1
S26361-F3552-E100	TPM 2.0 Module	1
S26361-F2567-E610	WINSVR 2019 DC 16Core OEM	1
FSP:GP3S60Z00NLSV2	TP 3y OS,9x5,4h Rt	1

Table 14 – PY TX2550 M5 Tower 8x2.5' (Medium Tower)

- X x PY TX2550 M5 Tower 8x2.5' (**Small Tower**)

Product no.	Name	Quantity
S26361-F3776-E121	ErP Lot9 configuration for 1 DIMM	1
S26361-F4082-E108	Intel Xeon Silver 4208 8C 2.10 GHz	2
S26361-F3849-E100	Cooler Kit 2nd CPU	1
S26361-F3694-E10	Independent Mode Installation	2
S26361-F4083-E332	32GB (1x32GB) 2Rx4 DDR4-2933 R ECC	2
S26361-F3266-E2	DVD-ROM 1.6" SATA	1
S26361-F5733-E240	SSD SATA 6G 240GB Mixed-Use 2.5' H-P EP	2
S26361-F5730-E112	HD SAS 12G 1.2TB 10K 512e HOT PL 2.5' EP	4
S26361-F5243-E11	PRAID EP400i	1
S26361-F5243-E155	FBU option for PRAID EP4xx	1
S26361-F5243-E100	TFM module for FBU on PRAID EP400i	1
S26361-F3953-E100	PLAN EM Blind Panel OCP	1
S26361-F4610-E4	PLAN CP 4x1Gbit Cu Intel I350-T4	1
S26361-F1452-E140	Region-kit Europe	1
S26361-F1790-E311	eLCM Activation License	1
S26361-F1790-E243	iRMC advanced pack	1
S26361-F2036-E100	ServerView Suite DVDs	1
S26113-F575-E13	Modular PSU 450W platinum hp	2
T26139-Y1740-E10	Cable powercord (D,..), 1.8m, grey	2
S26361-F3699-E20	Redundant power supply	1
S26361-F3552-E100	TPM 2.0 Module	1
S26361-F2567-E610	WINSVR 2019 DC 16Core OEM	1
FSP:GP3S60Z00NLSV2	TP 3y OS,9x5,4h Rt	1

Table 15 – PY TX2550 M5 Tower 8x2.5' (Small Tower)

10.2 Training

No requirement

11. Compliance

Fujitsu are accountable for compliance with specific regulations, dependant on the scope and nature of the proposed solution.

Section B – Infrastructure Design - Low Level

This section will be repeated for as many Infrastructure Design - Low Levels as required by the Infrastructure Design - High Level.

Section C – Appendices

Barenbrug Hyper-V
S_M_L 23OCT2020 - o

12. Glossary of Terms

Terms specific to this project are identified below:

Term/Abbrev	Definition
AD	Active Directory
AOD	Architectual Overview Design
AV	Anti-Virus
CPU	Central Processing Unit
DC	Data-Centre
DR	Disaster Recovery
GDC	Global Delivery CEnter
HBA	Host Bus Adaptor
HD	Hard Drive
HDD	HD Disk
HLD	High Level Design
HW	Hardware
FMO	Future mode of operation
JBOD	Just a Bunch of Disks
IIS	Internet Information Services
IP	Internet Protocol
iRMC	integrated Remote Management Controller
ISP	Internet Service Provider
ITSMC	IT Service Management Connector
LAN	Local Area Network
LAPS	Local Administrator Password Solution
LLD	Low Level Design
MAB	Microsoft Azure Backup
MMA	Microsoft Monitoring Agent
MPLS	Multi-Protocol Label Switching
NIC	Network Interface Controller
NTP	Network Time Protocol
NOC	Network Operation Center
OS	Operating System
PSU	Power Supply Unit
PTSG	Product Technical Support Group (FJ UK based)
RAID	Risks, Assumptions, Issues, Dependencies or Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RODC	Read Only Domain Controller
RPO	Recovery Point Objective

Term/Abbrev	Definition
RTM	Requirements Traceability Matrix
RTO	Recovery Time Objective
SAS	Serial Attached SCSI
SATA	Serial ATA
SDN	Software Defined Networking
SSD	Solid State Drive
SQL	Structured Query Language
VDU	Visual Display Unit
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
WAC	Windows Admin Center
WAN	Wide Area Network
WMI	Windows Management Instrumentation

Table 16 – Glossary

13. References

Ref	Doc Type	Document Reference	Description
Ref1	HLD/LLD	Azure infrastructure design	
Ref2	HLD/LLD	Infrastructure applications design	
Ref3	HLD/LLD	Network infrastructure design	
Ref4	HLD/LLD	Workplace design	
Ref5	HLD/LLD	Check_MK design	
Ref6			
Ref7			
Ref8			
Ref9			
Ref10			
Ref11			
Ref12			
Ref13			
Ref14			
Ref15			

Table 17 – Table of References

14. Document Control

Parameter	Value
Title:	Barenbrug Hyper-V Infrastructure Design
Component	Virtualisation, Windows Server, Hyper-V, Primergy
Summary:	High Level Design
Document Author:	Radis Nizamutdinov
Status:	Approved
Authorisation:	
Next Review Date:	
Distribution:	
Classification:	Commercial in Confidence

15. Change History

Version control			
VERSION	DATE	CONTRIBUTOR	CHANGE
0.1	23/10/2020	Radis Nizamutdinov	Initial draft
0.2	28/12/2020	Daniel Spelbos	Updates based on new server hardware list
0.3	28/12/2020	Radis Nizamutdinov	Updates based on new server hardware list
1.0	29/12/2020	Stefan van Aarle	Approved

Review control			
VERSION	DATE	REVIEWER	STATUS
1.0	20/01/2021	Stefan van Aarle	Approved

Please note it is important for users of this document that we have clear change history, to ensure updates to this document can be identified and tracked. This enables the impact on resultant documents and activities to be identified.