Infrastructure Design HLD
Microsoft Azure

Barenbrug

Document details

Version: 1.0
Status: Approved
Last Updated: 18/12/2020
Author(s): Radis Nizamutdinov

Contents

Section A – Infrastructure Design - High Level

1 Introduction

1.1 Document Purpose

This design documents the Microsoft Azure Infrastructure solution to meet Fujitsu's requirement to build greenfield infrastructure for Barenbrug. This will support the setup IaaS workloads in Azure and support them. It will also allow them to modernise their IaaS platform by leveraging PaaS or SaaS services in the future.

This design documents the virtualised infrastructure at high level. Further details if required will follow in a LLD or combined ID document

- It will detail the High level (HLD) elements of design
- It is a constituent part of a Service Design.

1.2 Scope & Requirements Traceability

1.2.1 Scope of document

Design of datacenter services in Azure to support and provide:

- Provision of a cloud hosting environment configured from Microsoft Azure to support multiple environments
- Deploy the required foundational infrastructure to support workloads in Azure
- Ensure network segregation between required environments
- Access control mechanisms to ensure connections to services hosted in the cloud remain secure
- IaaS services to host Barenbrug Servers
- Support existing and future operating systems that will be migrated to the Azure Datacenter(s)
- Provide Backup & Recovery services (Refer to Low Level Design)
- VPN connectivity configuration to Barenbrug infrastructure hosted at Azure Fujitsu CSP (Refer in more details to network design)
- Tagging of Azure resources for ease of administration and identification
- Data at rest encryption within Microsoft Cloud platform
- Azure Key Management System (KeyVault)
- Design of Azure Backup (LLD design or combined ID document)

Out of scope (although may be covered in other designs):

- Any hosting outside of Microsoft Azure (Legacy datacentre designs / documents)
- Design of the network outside of the Microsoft Cloud (Network design)
- On-premises ASR Configuration
- Design of the migration methods that will be used to migrate workloads to the Microsoft Cloud
- Design of Disaster Recovery failover of workloads running in Microsoft Azure. Although out of scope HA (High Availailability) groups can / will be deployed into Azure. These groups will be assessed based on application ability
- Design of Application architecture

- Design of cloud provisioning capability (To be considered for future mode of operation)
- Identity Management solution
- Cost Management Controls (Refer to Service Designs)

1.2.2 Requirements

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
R01	The Supplier shall perform backups of Customer Data in accordance with its obligations set out in the contract	Workloads and data hosted within Azure will be configured for backup with Azure Backup.
R02	Design for compliance with existing document storage and data management requirements and policies	Data stored on Microsoft Azure, in the public cloud, will only be accessible to BARENBRUG servers and devices.
R03	Implement the Supplier's standard procedures for performing storage management, in line with existing contractual requirements. Run books and service processes are typically internally referenced documents.	The IaaS VM's will use block storage on Microsoft Azure. Disks with include VM name to ensure they can be identified. Storage will be retained in line with data retention policies and erased when no longer required.
R04	Monitor and control storage services according to data management procedures in order to meet the Service Levels	Azure Monitoring will be implemented and will enable the revised KPI based service model which will be introduced subsequently.
R05	Allocate additional storage capacity as requested	Storage allocated to VM's can be increased in response to agreed change processes and agile working
R06	Provide storage tiers that provide different levels of performance based on those which are available within the Hosting services, where requested by the Customer.	BARENBRUG will have access to storage with different performance and availability characteristics to align with the different requirements of the various workloads.
R07	Provide Server Load Balancing for servers which Fujitsu currently provide Server Load Balancing that are in scope, using HA groups withing a single region.	High Availibility groups will be configured for those applications that support load balancing. Microsoft Azure will allow load balancers to be used at layer 4 and also at layer 7 (SSL offload and WAF possible) using the Application Gateway. The detail of Application Gateway use will be covered within a separate design.

1.2.3 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 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

1.3 Risks, Assumptions, Issues and Dependencies

1.3.1 Risks

Ref No	Risk	Probability	Impact	Action
R01	Identified VM type not available in selected Azure regions	L	L	Should the selected VM type not be available, an alternative VM with similar specification will be used.
R02	Azure Planned maintenance causes VM to reboot	M	H	Azure maintenance windows are notified by Microsoft and should be passed to BARENBRUG support teams by FJ. Critical servers should be placed in availability sets and load
R03	VPN connectivity is down between Barenbrug and Azure IaaS	L	M	A resilient VPN solution will be considered.
R04	Security Incidents on Azure platform, such as recent Spectre/Meltdown vulnerabilities	M	M	Where possible the use of availability sets with fault domains and update domains should allow service to continue without interruption during urgent patching activities on the Azure platform.
R05	User lifecycle management and cloud provisioning capabilities may be cumbersome and slow.	H	M	In the future, as an enhancement, user management could be streamlined through the use of Azure Active Directory Premium
R06	Cost Management of resources within Microsoft Azure	M	M	A commercial model is being agreed with Barenbrug. Refer to that document for costings.
R07	Azure Active Directory or other Microsoft controlled access and authentication	L	H	Risk to be accepted by Barenbrug and incorporated into the service model

Ref No	Risk	Probability	Impact	Action
	systems fail, preventing access.			
R08	Azure services and capabilities will change over time	H	M	Design will be based on Azure services publically available at the date of this document being released. Subsequent changes in capability may be incorporated under change control.

1.3.2 Assumptions

Ref No	Description
A01	New provisioned servers and services will use Windows Server 2019 as an operating system
A02	Azure backup solution will be used to backup IaaS infrastructure and native Azure monitoring tools will be leveraged for this purpose with further integration with Check_MK.
A03	An AD Connect will be deployed to sync on-premises AD users into Azure Active Directory (AADC).
A04	Microsoft Azure will be stable and available during the setup and during subsequent service
A05	All the technical deployment details are based on the current Azure platform capabilities. Microsoft may change this over time without notice, which may change how we deploy, provision or configure services within Azure.

1.3.3 Issues

Ref No	Description
I01	Adoption of Azure will drive new commercial and service models – those aspects will be outside the scope of this design

1.3.4 Dependencies

Ref No	Description	Dependency on
D01	Dependency on the Barenbrug's ISP to provide sufficient bandwidth on the VPN connection back into the BARENBRUG Azure environment. Please refer to Network design	Barenbrug
D02	Access to Azure Tenant(s) and subscription(s) available for build	Fujitsu

1.4 Constraints (Standards, Policies, Guidelines)

Ref No	Constraint
C01	All solutions and technologies deployed must be available and supportable at the time of design
C02	All designs will adhere to the Fujitsu IDBM process and governance
C03	Solution must be compliant with contractual storage and data management policies

1.5 Impact on Existing Infrastructure

The use of Microsoft Azure to host workloads is expected to have no impact on the existing infrastructure configuration for the legacy datacentre as a greenfield setup.

1.6 Gaps

There are no current gaps in the design or solution.

2 High Level Design

2.1 Architectural Summary

This design provides the building blocks for Barenbrug's resource deployment in Azure. The proposed solution will provide a foundation and other necessary security measurements and its governance for deploying resources in Azure.

Barenbrug's subscription(s) will follow the patterns and guidelines outlined in this document.

The following key requirements and decisions are addressed in this design document:

- Active Directory (AD) & Azure AD Strategy
- Naming convention for resources
- Tagging for Reporting and Billing
- Connectivity strategy from various Barenbrug locations
- Azure Network connectivity
  - VPN connectivity to on-premises resources
  - Virtual Network and Subnet segmentation
- Azure Security including Azure Security Center, RBAC, Azure Firewall etc.
- Public DNS strategy
- Azure Management strategy using Azure Monitor and also including patching, monitoring etc.
- Role Based Access Control and its strategy
- Server Migration using appropriate tooling recommendation
- Backup
- Extension of on-premises shared services such as Domain Controllers and Active Directory Domain services.
- Other Governance and Compliance tasks

2.2 Azure Solution Architecture

The use of Microsoft Cloud infrastructure in Azure for Barenbrug forms part of a Hybrid datacentre delivery, including on premises resources. For on premises resources based on Hyper-V – see Hyper-V infrastructure design. Microsoft Azure will allow servers to be created quickly and securely from cloud ready operating system images. The Microsoft Cloud also includes a range of other virtualised datacentre elements that can be used to enhance functionality.

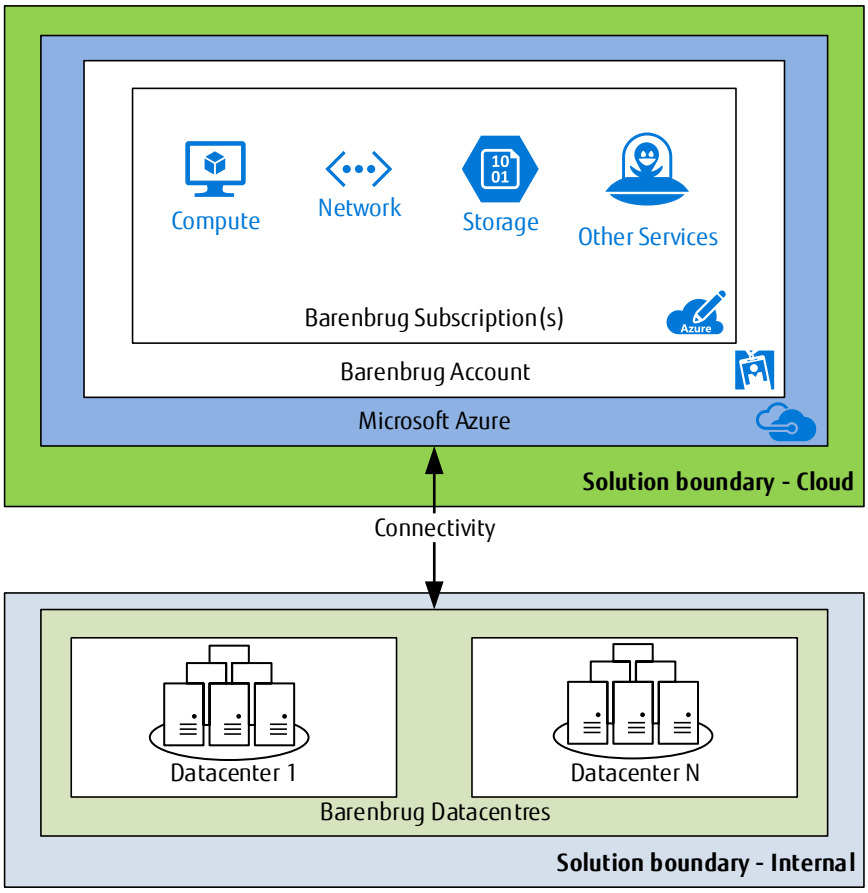

Figure 1 High-level Design

For Barenbrug, the capabilities of Microsoft Azure will be used in conjunction with deployments from internal datacentre. These platforms, when used together, will allow the business applications to function.

The Microsoft Azure infrastructure will use primarily IaaS components. The Barenbrug workloads are divided into three main geographic regions: West Europe, West US, Australia and into streams: Shared Services, Network and Security Services, Production, Test and DMZ. Each region will have it's own subscription per each stream. Each subscription will contain a number of VNETs/subnets, organised by function.

The following world map shows Barenbrug's inscope locations and Azure regions selected for workload running. Please see the link for full Azure Regions list.

The following diagram shows an example of the high level structure of the Microsoft Azure West EU region containing mentioned Subscriptions for Barenbrug. West US and Australia Central regions used in the configuration follows the same layout structure and will be connected to West EU via vNet peering of Networking vNets. Each Azure region will have Cisco Meraki vMX100 virtual appliance as a VNP concentrator for local region Barenbrug locations. Some subscriptions like DMZ and Test will be created on next stages of the project, for example, for corporate website workloads. Depends on future cloud workload West US and Australia Central Azure regions could be connected each other using vNet peering thus network ring will be created.

Figure 2 Barenbrug in scope locations world map and 3 Azure Regions selected

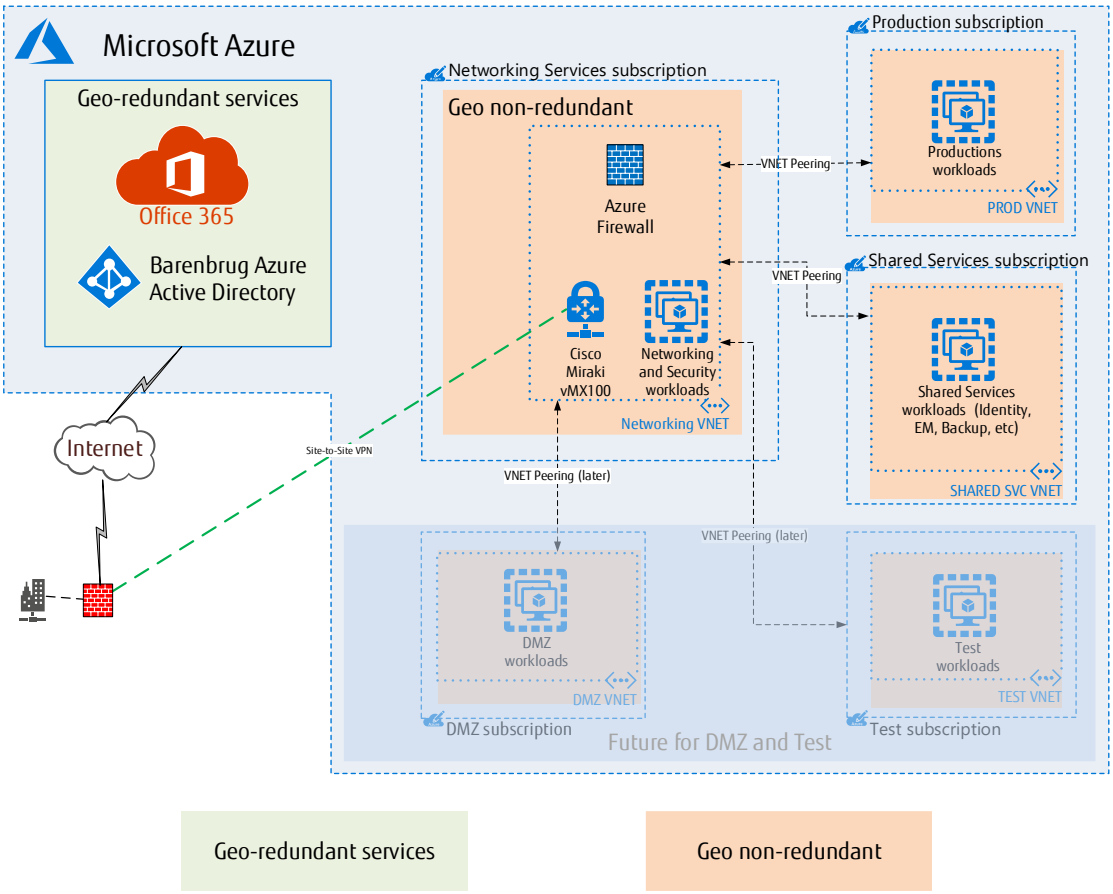

Figure 3 Azure Solution Architecture Diagram

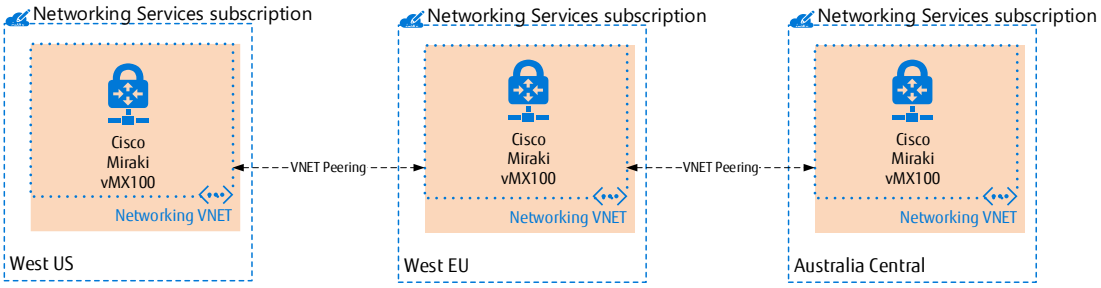

Figure 4 Azure Global vNet Peering

Fujitsu configures a Barenbrug tenant in the Azure public cloud in the West-Europe Zone (Amsterdam). In a later stage this could be mirrored to Northern-Europe, enabling high availability for the business critical systems of Barenbrug. The tenant is configured according to best practice of Microsoft, using a hub and spoke model on vNet level. The hub is the central segment where all traffic is routed through. Gateways, firewalls, jump boxes (Azure Bastion) are deployed in the hub. The spokes are vNets (segments) that hold the workloads of Barenbrug. Using this model unauthorized traffic straight to the workloads is prevented.
Fujitsu will also implement Azure backup. To keep costs down this will be the basic setup using only locally redundant (LRS) storage in each Azure region. This can be scaled out to a different region for business continuity (DR) and high availability reasons. Monitoring of Azure components is done through Azure Monitoring, automation through Azure Automation which is the automation standard for Fujitsu. Fujitsu enables the Azure CIS 1.1.0 baseline in Azure Security Center to harden the platform and the hosted systems.

Some supporting servers which provide infrastructure services, such as on-premises Active Directory will be build as well. The servers hosted within Microsoft Azure cloud will be a members of the new AD domain (principally Corp.Barenbrug.com). The Corp.Barenbrug.com AD Forest will be extended into the Hyper-V platform and FSMO roles will be in the cloud. Azure tenant AD will be Barenbruggroup.onmicrosoft.com. Azure tenant AD will be Barenbruggroup.onmicrosoft.com

As resources are deployed into Azure they will be named in line with a standard convention. Please refer to the Low Level design for further details

2.3 Azure Networking

Network Security Groups (NSG) are used to control access to each subnet. Typically this will be a whole subnet, except in the case of the DMZ subnet where the access list will be further reduced. The configuration of the NSG's is shown in the LLD.

Target design will use MS recommended hub-and-spoke topology with specifics of current security zone segregation.
This diagram below represents the hub and spoke resource group servers hosted within Microsoft Azure. Traffic from the VPN is terminated in the vMX100 Cisco Meraki appliance in the Networking VNET. It is passed through the firewall then over peering connection to target services in peered VNETs (production, test, shared VNETs).

Some services in Azure are only accessible on public IPs (SQL, Storage, KeyVault etc) so to avoid traffic going over public Internet Azure Service Endpoints (not shown on diagram below) will need to be deployed to allow access to these services from inside the VNET and so Microsoft back-bone.

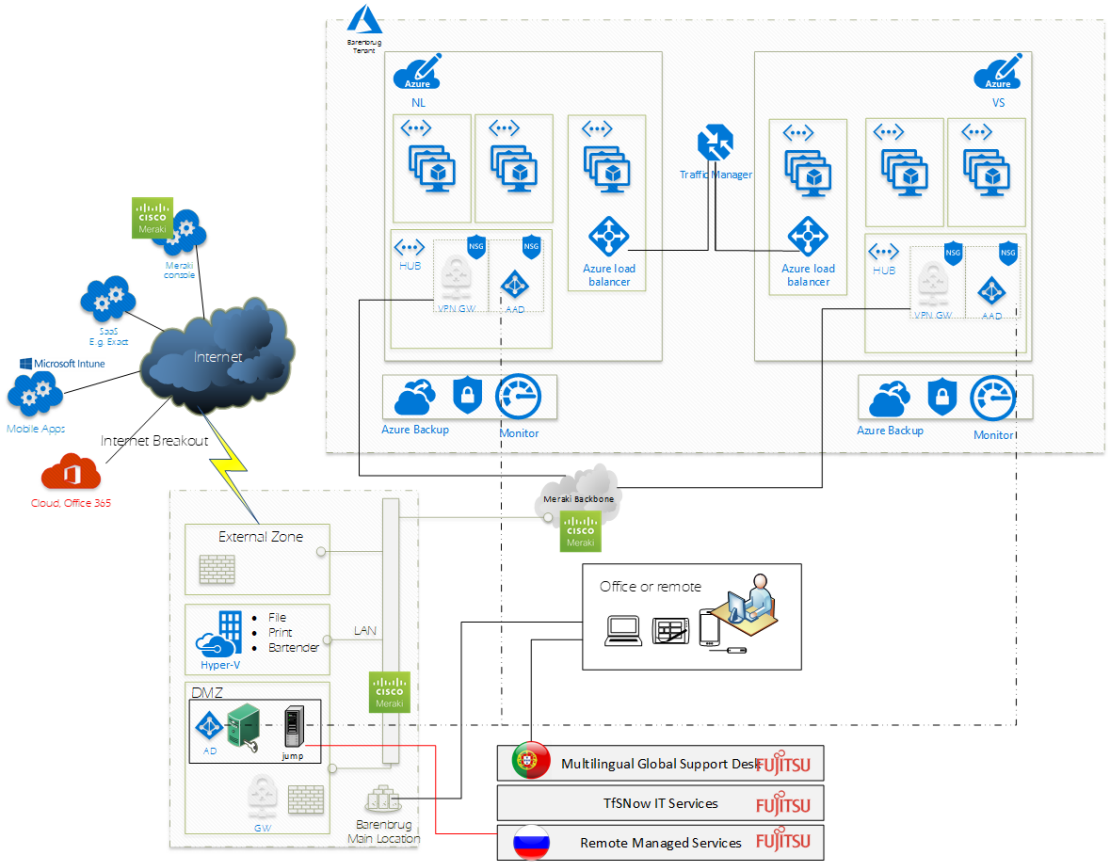

Figure 5 Azure Networking Diagram

2.4 Connectivity / Networking / VPN

Figure 6 below, shows an overview of the end-to-end layer 2 connectivity between the Barenbrug DC network and the Azure VPN circuits network and the other locations.

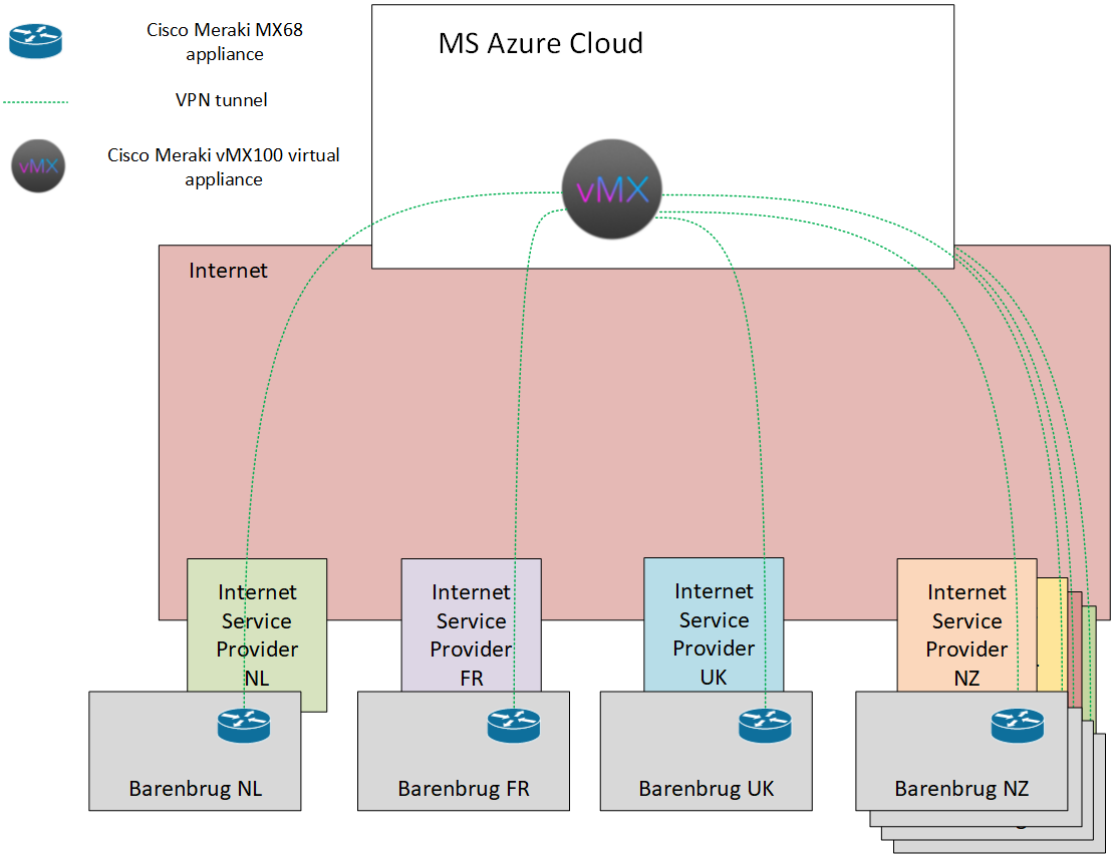

Figure 6 VPN Architecture Diagram

Barenbrug global network topology will follow hub and spoke model. Where hub will be Microsoft Azure public cloud site with Cisco Meraki virtual appliance deployed as VPN terminating device. Each Barenbrug physical office location will be acting as a spoke and have VPN connection initiated by local Cisco Meraki MX appliance to the hub.

VPN connections will be using Internet lines as transport for encrypted communications. VPN tunnel will be initiated and terminated on Cisco Meraki MX security appliances. Every location will have VPN tunnel only to the hub. Hub will aggregate and terminate VPN connections from every remote site.
For more info please see Network design.

3 Design Decisions

The following design decisions have been taken during the detailed design process. The Barenbrug / Fujitsu Azure design principles has also cascaded some requirments which have been considered during this phase and included, please refer to that document for further details, see the reference section for information

Component	Decision	Rationale
Regions	Barenbrug will use Azure Datacentres in Europe, USA and Australia.	Whilst Azure is also available in UK Datacentres, the cost is higher than European Datacentres. West EU will cover EMEIA region, West US will cover AMER region and Australia Central – APAC.
Primary Region	The West EU region for the Production, Test and Shared Services environment	Azure services required are all available from the West EU region.
Subscriptions	The following subscriptions will be used on Azure IaaS platform. Networking, Production, and Shared Services. Required network security posture can be achieved through the use of Network Security Groups and User Defined Routing when Azure Firewall or other filtering (e.g. Checkpoint NVA) appliance is used.	This subscription model will logically isolate production workloads from non-production. External facing workloads will be hosted within these subscriptions and secured through the use of Network Security Groups which will be assigned to subnets and will be used to separate subnets. The use of a shared services VNET to hold common resources will reduce overall hosting costs in comparison to deployment of shared services (AD, Security etc) in each VNET.
Server Availability	Availability sets or Availability Zones will be used to group and protect VM's deployed in Azure. As each Barenbrug application is migrated to Azure in the later project stages, if the application contains more than one server providing the same function then an availability set or Availability Zones will be used. Domain controllers will be added to availability zonez as well.	An Availability Set is a logical grouping capability within Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed within an Azure datacentre. Azure ensures that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a failure occurs within the Azure platform, only a subset of VMs are impacted. This idea is even expanded with Availability Zones when different datacenters (power, cooling, networking) are used.
Cisco Meraki vMX100 Virtual Applience, Azure Load Balancer, Public IP Address (PIP)	vMX100 will be in One-Armed Concentrator mode. Use zone-redundant SKUs	This is the only supported configuration for MX appliances serving as VPN termination points into Azure. Zone-redundant SKUs ensure that these services are deployed redundantly over Availability Zones
Storage	Managed disks will be used for all production storage except for diagnostic storage volumes. It has been agreed that Production to be on standard disks. For critical workloads premium disks could be used after agreement.	Storage accounts have associated capacity and performance limits. Managed disks help to reduce complexity and avoid performance bottlenecks. It has been agreed that Production and non production to be on standard disks. Fine tuning may take place post migration if indicated by actual iops consumption.
Network Security Groups	Network security groups will be used to segment subnets and servers as required. During migration NSG's will operate at a subnet level.	Network security groups can be associated to subnets or individual network interfaces attached to VMs. When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

Component	Decision	Rationale
Security Zones	VNET and Subnet level isolation will be used to separate Azure virtual machine workloads.	To achieve the required network security posture, Azure Firewall (or NVAs) and Network Security Groups will assigned to subnets and will be used to separate subnets as required.
Routing Tables	Isolated subnets will use user defined routing to control flow of network traffic.	Where a subnet is isolated, user defined routing will be configured to send all traffic towards virtualised firewalls within Azure.
Networking	Create VNETs for different purposes (Production, Test, Shared, Networking/Security)	Use hub and spoke topology for Prod/Test/Shared/Network.
Networking	Within the VNet multiple subnets will be defined	To allow granular yet manageable (for NSG) server grouping
Management groups and RBAC	Use separate management groups and resource groups for different management domains (e.g. networking/per application/shared service)	Enable granular Azure RBAC and Azure Policy on Management Group, Subscription and Resource Group basis
Connection to core network	Cisko Meraki vMX100 Virtual Applience will be created to connect On-Premise network. IPSec site-to-site VPNs will be used for 3rd party vendors into the exisiing legacy datacentres	Cisko Meraki blueprint solution is used on premises sites
IP Addressing	Private IP addresses will be manually assigned to servers hosted within Microsoft Azure.	While Azure supports dynamic IP address allocation to network interfaces we will use static assignment to allow for control to be maintained of the IP address schema.
Network Load Balancers	Azure Load Balancer is a Layer 4 (TCP, UDP) load balancer can be used where required by the application. A basic load balancer is free. Also available is the Microsoft Azure Application Gateway which offers Layer 7 load balancing.	Applications will vary in their requirements for load balancing. The Microsoft Azure platform offers good options for load balancing services.
Backup Technology	Servers in Microsoft Azure will primarily use Azure backups. The design will retain Commvault for legacy systems and adopt Azure Backup for the Azure hosted workloads, refer to design principle 4.10	Microsoft first.
Azure Resource Groups	Resource Groups will be organised per Application per subscription.	An application centric organisational structure will allow all elements of a customer facing application to be grouped together to allow for ease of management. (Note there some already in use resource groups which group resources based on type)
Resource Tagging	Each object within Azure will be tagged to allow for management and traceability.	Each object will be tagged with application and support information. This will ease management and enhance traceability.
Design documentation	Design will be flexibile for additional services and will support the extension and/or shift of services and resources to Azure.	If additional services need to be added to the Azure platform during the discovery phase of a site (e.g. file services, application services, website, etc.), the design can comprise these services. Of course, the implementation of additional services are out of scope.

4 Non-Functional Requirements

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

4.1 Availability & Resilience

Hours of service are defined in the current contract which will be amended to reflect the capabilities of the Azure platform and hence the service responsibilities of Fujitsu as distinct from Microsoft.

The Barenbrug Service design outlines Fujitsu's obligations in providing support, availability and resilience outside of normal service hours. A Service design is being drafted and must be signed off before a server can be migrated and handed into supported and made live.

4.1.1 Availability

Availability statements for the Microsoft Azure platform for components considered within this cloud design. These are aligned to Microsoft Azure platform availabilities , adopted for this design, notwithstanding any changes by Microsoft. Please note that the legacy components will have other availaibility.

Item		
Compute/other zone-redundant services	Two or more VM deployed to different Availability Zones. Zone-redundant services (e.g. Load Balancer) replicate your applications and data across Availability Zones to protect from single-points-of-failure.	99.99%
Compute	Two or more VM instances deployed in the same Availability Set, connectivity to at least one instance	99.95%
Compute	Single Instance Virtual Machine using premium storage for all Operating System Disks and Data Disks	99.9%
Storage	Successfully process requests to read data from Read Access-Geo Redundant Storage Accounts, provided that failed attempts to read data from the primary region are retried on the secondary region	99.99%
Storage	Successfully process requests to read and write data from Locally Redundant Storage (LRS), Zone Redundant Storage (ZRS), and Geo Redundant Storage (GRS) Accounts	99.9%
RPO		
RTO		

4.2 Service Continuity (Disaster Recovery)

The production platform for Barenbrug will, as well as TEST be hosted in the Microsoft Azure Cloud in the West Europe, West US and Australia Central regions. Azure Site Recovery can be utilized case by case when regional redundancy is required with [semi-]automated failover capability.

4.2.1 Backup and Restore

Servers deployed within Azure for Barenbrug will be moved to Azure Backup and will be documented in the relevent LLD sections

4.3 Capacity and Performance management

As Microsoft Azure is a public cloud offering there is generally always capacity available within Azure should expansion and growth require it. Virtual machines and storage can be easily expanded

through the features of the Azure Cloud platform. Azure Monitor will be deployed within the Azure environment for reporting and management.

Capacity Management for clouds deal with limiting uncontrolled resource usage (yet balanced for agility of business) using cloud governance measures and ensuring built-in limitations for cloud resources are not breached.

Governance is described in "Governance" chapter below.

Dealing with limitations is performed per resource-type basis consulting with published limitations in Azure docs (https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits).

From the beginning we need to setup following objects to be monitored for resource limits:

- Azure Firewall;
- Rule number/NSG;
- Storage account limits (for un-managed disks, managed disk are taken care by MS itself);
- User-defined routes per UDR (route table);

If Azure Monitor using Log Analytics is setup then also Log Analytics usage need to be configured for limiting amounts of data stored, leaved uncontrolled it can produce lots of costs.

During implementation of new services Azure good practices and limits need to be evaluated and possibly new capacity monitoring rules / cloud resource usage rules / governance policies developed.

4.3.1 Growth and Sizing (Current and Predicted)

The server footprint on the Barenbrug estate may rise and fall as different projects commission new systems and decommission legacy systems, such adjustments will be managed under Change Control. Overall, Barenbrug intend to rationalise systems over time and adopt a SaaS / PaaS approach – such changes will be outside the scope of this project. Existing sizing data is provided in the LLD

4.3.2 Enterprise Management

The Microsoft Azure Cloud is a managed platform and therefore includes Enterprise Management of the underpinning infrastructure. The Enterprise Management of BARENBRUG workloads running on Azure will be facilitated by Azure Monitor. There is a separate design for Azure Monitor as deployed for BARENBRUG.

4.3.3 Remote Support

Remote support of the Microsoft Azure resources which make up the Barenbrug infrastructure is via the Azure Portal. This is a public interface which is available via the internet. Access to connect to deployed servers within Microsoft Azure will be provided via the Barenbrug network. Jump servers will be deployed in the Azure subscription to perform administative tasks as well.

4.4 Supportability

4.4.1 Support Teams

The Azure infrastructure within the configured subscriptions for Barenbrug will be supported by the GDC support team, as defined in the Service Design (see References 9)

The supported Azure Subscriptions are listed in section **Error! Reference source not found.** above.

4.4.2 Support Contracts

Microsoft Azure 4th line support will be provided by the Fujitsu Product support group with escalation to Microsoft, utilising Fujitsu's Gold Partner status, as required.

5 Security

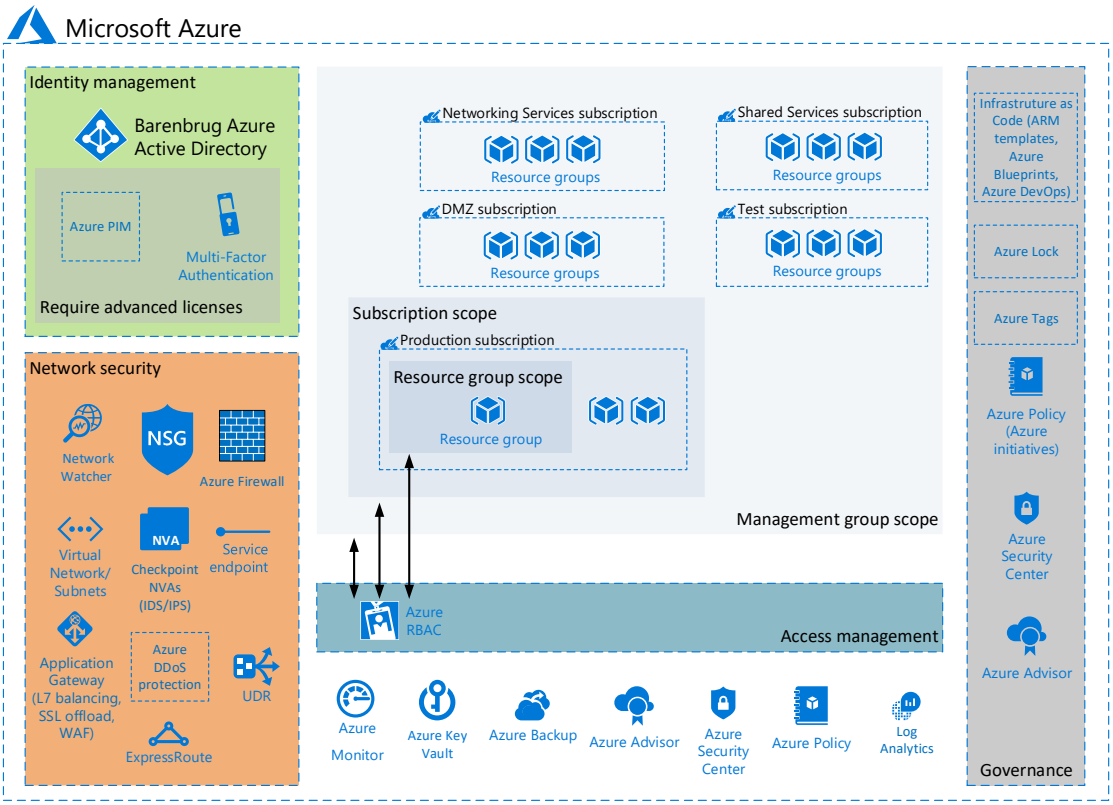

Figure 7 Azure Security and Governance Architecture Diagram

The Barenbrug infrastructure deployed on the Microsoft Azure public cloud platform will inherit security characteristics of the platform. Microsoft Azure conforms to the new international cloud privacy standard, ISO 27018.

5.1 Physical Access

Physical security is outside the scope of this design as the infrastructure deployed will be within a virtualised cloud infrastructure and outside the control of Fujitsu.

5.2 Network

5.2.1 Network Traffic

Connection between Barenbrug core network and Microsoft Azure will be via site-to-site VPN connection via Cisko Meraki vMX100 Virtual Applience running in West EU region. This connection will be sized according to the workloads to be migrated to Microsoft Azure. For more info see Network design.

5.2.2 Network Segmentation

Azure Network will be split on a few Virtual Networks(VNET) resources one for each type workload to isolate workload from each other as VNET is fully isolated routing boundary. Each VNET will be logically segmented by subnets that aggregate servers into a logical group. Logical segmentation will provide the possibility for network macro-segmentation though the Azure Firewall or NGFW.

5.2.3 Network Protection/Service Endpoints

All PaaS services that are going to be deployed and require connection with the resource within the VNET must be integrated with the VNET via Service Endpoint. Virtual Network Service Endpoints extends the virtual network private address space and the identity of VNet to Azure services to secure Azure services such as Storage and PaaS SQL Database which has Internet facing IP addresses

5.2.4 Network Security Groups

Network Security Groups will be used to filter traffic between subnets and VNETs. NSG will be applied only on the subnet level to simplify administration and because there are no requirements for micro-segmentation between subnet.

5.2.5 Application Security Groups

Application Security Groups will be used to provide security micro-segmentation within the subnet and VNET as well as simplify network traffic filtering on the NSG level.

5.2.6 Network Watcher

Azure Network Watcher is a cloud-based service that monitors and diagnose networking issues, provide nsg group flow logs, diagnose connectivity issues, ability to define next hope and more. Logging and auditing of this service will be limited by default Azure volumetric.

The Azure Network Watcher will be enabled for all azure subscription.

5.2.7 Firewall

At the beginning of the project, the Azure Firewall will be used to protect, filter network traffic between the internal network segment. At the later stage, it is recommended to implement NGFW that will be used for inter regions traffic filtering.

5.2.8 Application Gateway

Application Gateway is Layer 7 Load balancer that has WAF and SSL offload functionality. One instance of Infernal application gateway will be deployed within the Share Network Services VNET to provide SSL offload and WAF functionality for internal services if needed on next project stages.

5.2.9 Public IP/External Connection

Azure Public IP provides an endpoint for connection from the external network, internet. Direct access to the Azure Internal Network from the internet is not allowed, consequently, Public IP usage will be prohibited all VNETs except shared network VNET. This will be enforced by Azure Policy

5.2.10 DDoS Protection

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Azure DDoS has two service tiers: Basic and Standard.

As all Public IPs will be concentrated within one VNET, it is recommended to consider Standard DDoS tier for this VNET. All other VNET will have a default, Basic, protection that is free and enabled by default.

- **Basic**: Automatically enabled as part of the Azure platform. Always-on traffic monitoring, and real-time mitigation of common network-level attacks, provide the same defenses utilized by Microsoft's online services. The entire scale of Azure's global network can be used to distribute and mitigate attack traffic across regions. Protection is provided for IPv4 and IPv6 Azure public IP addresses.

- **Standard**: Provides additional mitigation capabilities over the Basic service tier that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard is simple to enable, and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses associated to resources deployed in virtual networks, such as Azure Load Balancer, Azure Application Gateway, and Azure Service Fabric instances, but this protection does not apply to App Service Environments. Real-time telemetry is available through Azure Monitor views during an attack, and for history. Rich attack mitigation analytics are available via diagnostic settings. Application layer protection can be added through the Azure Application Gateway Web Application Firewall or by installing a 3rd party firewall from Azure Marketplace. Protection is provided for IPv4 Azure public IP addresses.

Further details are available at https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

5.2.11 Routing Control

Route Tables will be used to control traffic between subnets and VNETs as well as force traffic flow with Azure Firewall or NGFW. Route Tables will be applied for each subnet within the Azure environment.

5.3 Compute & Storage

5.3.1 Anti-virus and Anti-malware approach

Due to project scope cut off Security management is not included now. Selected O365 license does not support Windows Defender ATP for PCs and off Azure workloads. Build in Windows Defender still can be used for off Azure workloads, for PCs configuring via Microsoft Intune. Microsoft Antimalware for Azure Cloud Services and Azure Virtual Machines could be enabled on later project stages as well.

5.3.2 Encryption

5.3.2.1 Data at rest

Data at rest represents any data not being actively moved or processed, including files, databases, virtual machine drives, PaaS storage accounts, or similar assets. Encrypting stored data protects virtual devices or files against unauthorized access either from external network penetration, rogue internal users, or accidental releases.

IaaS virtual resources will be secured through virtual disk encryption using cryptographic keys stored in the Azure key management system.

PaaS storage and database resources will be enforced with data encryption at rest.

Encryption for data at rest also encompasses more advanced database encryption techniques, such as column-level and row level encryption, which provides much more control over exactly what data is being secured. That kind of encryption is not foreseen in this design document until PaaS is adopted

5.3.2.2 Data in transit

Data in transit is data moving between resources on the internal, between datacenters or external networks, or over the internet.

Encrypting data in transit will be done by requiring SSL/TLS protocols for traffic. Traffic transiting between cloud-hosted resources to external network or the public internet should always be encrypted.

Network connectivity between Azure and on-prem will go thought a dedicated WAN connection that is VPN route. Traffic within the Azure will not be encrypted.

All Azure Storage Accounts will be configured to require TLS connection. All other PaaS service offering will be protected where possible by native compatibilities.

5.3.2.3 Data in use

Encryption for data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. Use of technologies such as full memory encryption, enclave technologies, such as Intel's Secure Guard Extensions (SGX). This also includes cryptographic techniques, such as homomorphic encryption that can be used to create secure, trusted execution environments.

Data encryption in use for IaaS components of the Azure infrastructure will not be applied. It should be considered where applicable for the Azure PaaS offerings.

5.3.3 Security patching

Azure servers will be patched using Azure Update Management. See REF9 for Azure Update Management design.

5.3.4 Operating System Hardening

All Azure Virtual machines will have the current Operating System image and hardening settings. It is not foreseen to perform OS or Build adjustment during migration

5.3.5 Vulnerability management

Vulnerability management of Azure components and Azure virtual machines will not be provided

5.3.6 Key Management

Key management system is critical part of every organization as it provides ability to create and store cryptographic keys, important passwords, connection strings, and other IT confidential information in the appropriate manner.

The Cloud Native Key Management system will be implemented within the Barenbrug Azure infrastructure. The solution will be based on the Azure Key Vault service offering and used only within Azure Infrastructure. The Software based offering of Azure Key vault will be used.

The Azure Key Vault will be used for VM encryption, Deployment Automation as well as for storing cloud native passwords.

The Azure Key Vault will be connected to the Virtual Network via Service Connection Endpoints and connection from external network will be limited to the trusted IP addresses.

Separate RBAC will be applied to Data and Management plane

Refer to the LLD for further details

5.4 Identity

The Hybrid Identity approach will be used within the Barenbrug environment where on-premise Active Directory Domain Services are integrated with Azure AD via Azure Active Directory Connect tool. Azure AD Connect will synchronize require object to Azure AD.

Users authentication to the Azure AD will be performed though the on-premise Active Directory, Azure AD Connect will be used, please see O365 design for more info. In additional to this, password hash synchronization will be enabled in Azure AD Connect tool. User Authorization for Azure will be performed by Azure AD based on the user's group membership.

5.4.1 User Access

The Microsoft Azure portal will be used by Fujitsu support teams to access the deployed infrastructure for Barenbrug. A Role Based Access Control policy will be used to allow those support teams, to have one of three levels of access per Azure subscription as required for their role. These will be;

- Administrator, where resources can be added and removed
- Operator, allowing users to stop and restart resources
- Read Only giving users the ability to review the configuration but make no changes.

Refer to the LLD for further details.

5.4.2 Azure Active Directory

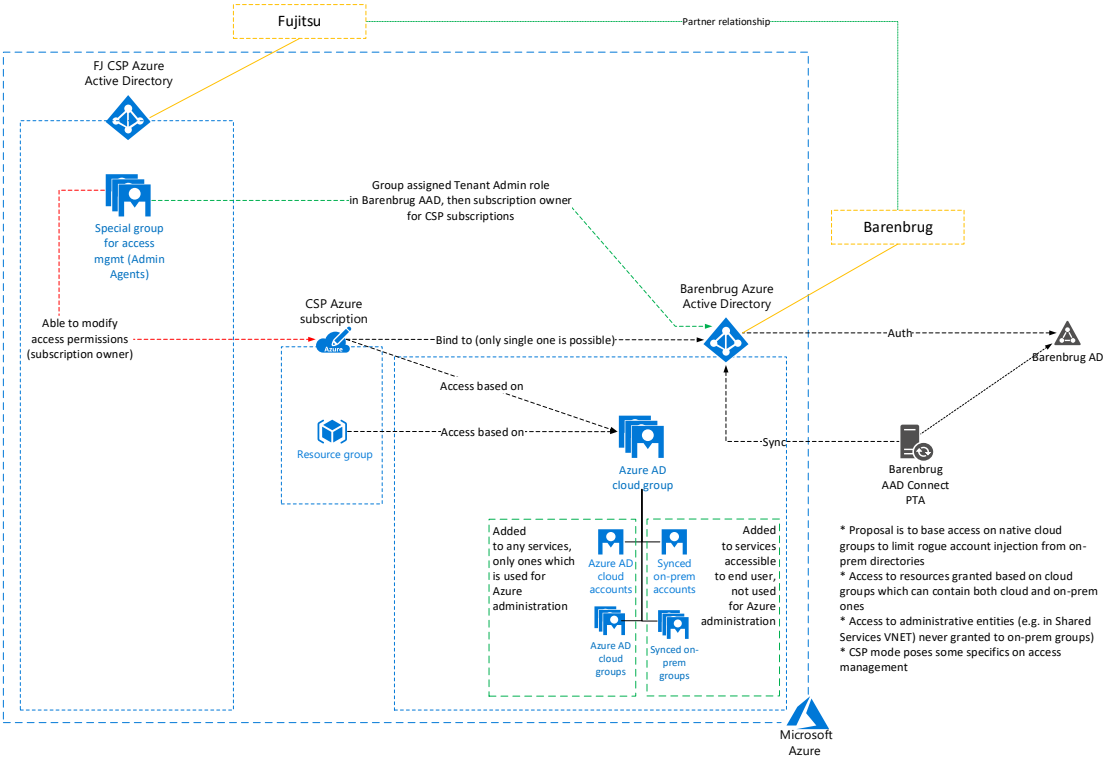

Figure 8 Azure Active Directory Diagram

Azure subscriptions will need to bind Barenbrug Azure AD:

- Proposal is to base access on native cloud groups to limit rogue account injection from on-prem directories;
- Access to resources granted based on cloud groups which can contain both cloud and on-prem ones (hybrid approach);
- Access to administrative entities (e.g. in Shared Services VNET) never granted to on-prem groups;
- CSP mode poses some specifics on access management .

5.4.3 Administrative Accounts

All accounts that have administrative privileges in the Azure Platform must be created directly in Azure AD and have onmicrosoft.com domain suffix. These accounts are required to separate administration boundaries between on-prem environments and Azure platform that will eliminate risks of impact on both environments in case of account compromisation. All future admin account to be approved under change control (CAB)

5.4.4 Multi-Factor Authentication

It is strongly recommended to enabled Azure Multi-Factor Authentication for all accounts that have administrative privileges and might have significant impact on the environment if their account is compromised.

Azure MFA is enabled only for all Azure Administrative accounts. For users part please see M365E3 design REF4.

5.4.5 Azure AD Privileged Identity Management

Azure AD Privileged Identity Management is a service that allows manage, control, and monitor access to important resources in the cloud. The Azure AD PIM provides possibility to follow Just-in-Time(JIT) administration approach with approval process for Azure resources as well as some other PaaS offerings.

It is strongly recommended to protect high privilege roles with the Azure PIM.

At the time of the writing, Azure PIM will not be implemented.

5.4.6 Azure Active Directory Identity Protection

Azure Active Directory Identity Protection Azure IP provides a possibility to detect abnormal behavior for the accounts and apply risk-based condition access polices that can protect environment in case of account compromisation.

It is strongly recommended to protect all account that have administrative privileges in Azure.

At the time of the writing, Azure IP will not be implemented.

5.4.7 Conditional Access

Conditional Access polices allow to force additional security measure for the accounts that are trying to do some abnormal actions or force pre-defined set of security requirements during sign-in from unknown locations.

At the time of the writing, Azure AD Conditional Access will not be implemented. For user access part – please see M365E3 design REF4.

5.4.8 RBAC

Role-Based Access Control for Azure Platform will be implemented based on the Azure AD Groups. A Resource Group will be an administration boundary on which access will be delegated.

Usage of Azure AD groups in RBAC provides flexibility of the access delegation as it can contain as members not only Azure native objects but also object that are synchronized from the on-premises Active Directory

5.5 Logging & Monitoring

5.5.1 Logging

At the time of the writing, there is no cloud-native SIEM solutions within the Azure that can be utilized. Azure Sentinel is currently in the public preview and can be considered later when will be in GA.

At the time of the writing, Azure Log Analytics free tier will be used in case of emergency. The free tier is limited to 500 MB per day not more, after reaching this limit no new events will be saved to the store.

Azure Activity Logs will be stored 90 days that is default retention policy in Azure platform for such events. Due to absent of SIEM solution, all other Azure Platform logs will be also stored as per default Azure values and will not be integrated with other solutions.

5.5.2 Monitoring

Azure Monitor, which now includes Log Analytics and Application Insights (VM insights is in preview), provides sophisticated tools for collecting and analyzing telemetry that allow you to maximize the performance and availability of your cloud and on-premises resources and applications. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Azure Monitor will be primary metric collection and reporting system. It will stay as monitoring tool for Check_MK integration with further Check_MK-ITSM integration.

Azure Monitor collect data in Log Analytics which is charged based on usage (https://azure.microsoft.com/is-is/pricing/details/monitor/), additional services like ASC Standard tier cost 10-15$ per VM instance.

Log Analytics usage imply lots of data stored in Log Analytics workspaces. Enabling data collection must be made with care and recommendations examined (https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-cost-storage) and limited if it is confirmed that data amounts breach some cost limits.

Application performance monitoring is possible using Application Insights. Application Insights require installation/instrumentation to be made for supported .Net/Java/Node.js applications. See more here (https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview).

Integration of the Azure Monitor with other Azure Offerings are not foreseen as part of the project.

6 Governance

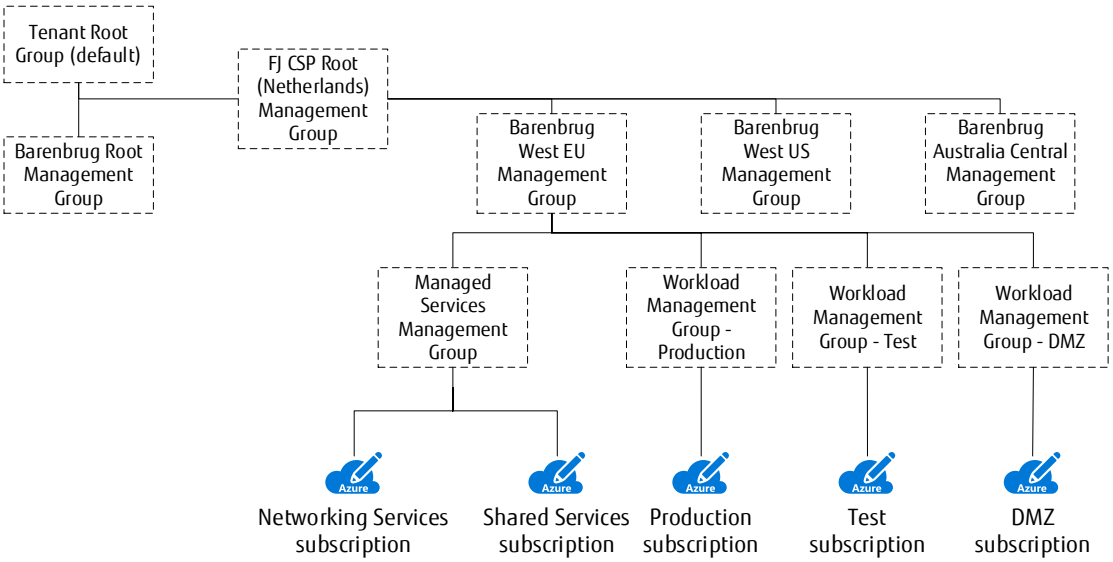

Figure 9 Azure Management Groups Diagram

Governance in Azure is based on Azure Policies (and groups of policies are called Azure initiatives) which can be applied at resource group, subscription or management group level. Management group structure is shown on diagram above.

6.1.1 Azure Policy and Azure Initiatives

Different Azure Policies will be created to lock or force specific requirements for Azure platform. All of this Azure polices will be aggregated to Azure initiatives and applied on the Management Group and Subscription levels.

This implementation will enforce general rules for all subscriptions as well as provide granular policy enforcement for each subscription that provides flexibility in terms of governance

6.1.2 Azure Lock

Azure Resource Lock provides possibility to prevent deletion of the resource by putting Lock on it. There are two types of Azure Lock: Read-Only and Delete. The Azure Lock Delete will be applied for all Resource Groups in all subscription to prevent resource deletion. The Lock will be applied to all resource within the Resource Group

6.1.3 Azure Tags

Azure Tags will be used to logically organize resources. Each tag consists of a name and a value pair. Tags will be applied to Resource Groups and Resource itself.

6.1.4 Deployment and Resource consistency

Azure Blueprinting and Azure RM templates will be used for deployment. Both provides declarative deployment model.

6.1.5 Secure DevOps Toolkit

The "Secure DevOps Kit for Azure" is a collection of scripts, tools, extensions, automations, etc. that caters to the end to end Azure subscription and resource security needs for dev ops teams using extensive automation and smoothly integrating security into native dev ops workflows helping accomplish secure dev ops.

The Secure DevOps Toolkit will be run in the Audit mode for reporting purpose only. All required remediation will go through the change management process

6.1.6 Azure Advisor

Azure Advisor will be used to see vendor recommendation for cost optimization.

6.1.7 Azure Security Center

The Azure Security Center provides a unified view of the security status of resources across environment in addition to advanced threat protection. The baseline capabilities of Azure Security Center (free tier) provides assessment and recommendations that will enhance security posture. Its paid tiers enable additional and valuable capabilities such as Just In Time admin access and adaptive application controls (whitelisting).

As starting point, it is recommended to enabled Standard Tier for shared VNET service as it has publicly available footprint. There is a cost for the relevant toolset and data storage. It will be started with Azure Security Center free and it could be upgraded later.

6.1.8 Azure Cost Management

Azure Cost Management is not part of this design. Azure costs are subject to the Fujitsu and Barenbrug commercial agreement.

7 Implementation, Testing and Validation

7.1 Testing

The approach to acceptance testing encompasses three distinct phases:

- Unit Test
- Integration (System) Test
- Operational Acceptance Testing
- Define Bring Into Service documentation and approval

7.1.1 Unit Test

Unit Test is concerned with ensuring that the hardware and software components are established and running satisfactorily within the component's own localised environment. This includes testing access to the components for configuration and customisation purposes. This set of testing will take place as part of the build phase.

7.1.2 Integration Test (System Test)

Integration Test is concerned with establishing the end-to-end functionality of all the components within the specific system concerned. This encompasses testing connectivity and service functions between the various components of the system and to any external components that may be involved.

7.1.3 Operational Acceptance Testing

Operational Acceptance Testing is concerned with proving to Fujitsu that the system is fit for purpose and fulfils its intended functions and is supportable. This will include ensuring that the individual service elements and use cases, which the system was designed to fulfil, work as specified and provide the performance and capacity required to scale into production. This will take place prior to any User Acceptance Testing done by Barenbrug and the Fujitsu support teams.

7.2 Implementation

The implementation of the Microsoft Azure infrastructure for Barenbrug will be carried out in the following, high level order;

- Ensure implementation team have sufficient permissions
- Create Subscriptions
- Create VNets
- Create Subnets
- Create Azure Firewall
- Create Cisco Merki vMX100 Virtual Applience
- Create Diagnostic Storage Accounts
- Create Virtual servers within Azure
- Assign additional storage to virtual servers
- Assign network security groups to subnets
- Modify existing Network Security Groups
- Change User Defined Routing

8 Bill of Materials

There is no bill of materials for this design as this design documents the infrastructure framework for the use of the Microsoft Azure Cloud. Microsoft Azure is billed monthly on an operational expenditure model. This includes all services provided from Azure such as servers, licenses, storage, network devices and connections.

9 References

All design reference material can be found in the SharePoint library.

Ref	Document Ref	Description
REF1	TBA	Requirements Catalogue and Traceability Matrix (RCTM)
REF2	Commercial model	
REF3	TBA	Barenbrug Service Design
REF4	Workspace design	HLD/LLD
REF5	Check_MK design	Azure Monitor will be integrated with Check_MK
REF6	To be developed	HLD/LLD
REF7	Hyper-V infrastructure design	HLD/LLD
REF8	Network infrastructure design	HLD/LLD
REF9	Infraaps design	HLD/LLD

10 Glossary of Terms

Specific terms to this project are identified below:

Term/Abbrev	Definition
AD	Active Directory
API	Application Programming Interface
AZ	Availability Zone
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DR	Disaster Recovery
GDC	Global Delivery Centre
GPO	Group Policy Object
HLD	High Level Design
LLD	Low Level Design
NSG	Network Security Group
NTP	Network Time Protocol
OS	Operating System
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
SCCM	System Centre Configuration Manager
SCOM	System Centre Operations Manager
SLA	Service Level Agreement
SQL	Structured Query Language
SSL	Secure Socket Layer
TAD	Technical Architecture Document
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
UMI	Unrestricted Management Infrastructure
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine

11 Document Control

Parameter	Value
Title:	Microsoft Azure Infrastructure Design for Barenbrug
Component	Infrastructure
Summary:	Design of the Microsoft Azure Cloud infrastructure to support the migration of services from Barenbrug to Microsoft Cloud hosting.
Document Author:	Radis Nizamutdinov
Status:	Draft
Authorisation:	TBD
Next Review Date:	TBD
Distribution:	
Classification:	HLD LLD ID

12 Change History

Version control			
VERSION	DATE	CONTRIBUTOR	CHANGE
0.1	19/05/2020	Radis Nizamutdinov	Initial Version
0.2	25/05/2020	Radis Nizamutdinov	Azure regions vmx100 corrected, map diagrams added
0.3	07/10/2020	Radis Nizamutdinov	Minor changes as per review
0.4	12/10/2020	Radis Nizamutdinov	Minor changes as per review
1.0	15/12/2020	Radis Nizamutdinov	Minor changes as per review

Review control			
VERSION	DATE	REVIEWER	STATUS
0.2	01/10/2020	Stefan van Aarle, Barenbrug	Draft comments after design workshop meeting
0.3	09/10/2020	Daniel Spelbos, Fujitsu	Comments after review
1.0	18/12/2020	Stefan van Aarle, Barenbrug	Approved