Table of Contents

[1 Microsoft Azure 4](#_Toc36653422)

[1.1 Requirements 4](#_Toc36653423)

[1.2 Azure High-Level Design 4](#_Toc36653424)

[1.2.1 The Virtual Data Center 4](#_Toc36653425)

[1.2.2 Terminology 4](#_Toc36653426)

[1.2.3 VDC Concepts 5](#_Toc36653427)

[1.2.4 Infrastructure-as-Code (IaC) 6](#_Toc36653428)

[1.2.5 Governance 7](#_Toc36653429)

[1.2.6 Management 10](#_Toc36653430)

[1.2.7 Security Management 11](#_Toc36653431)

[1.2.8 Edge Data Centre (EDC) 12](#_Toc36653432)

[1.2.9 VDC Instance Design 12](#_Toc36653433)

[1.2.10 Domain Controllers Spoke 14](#_Toc36653434)

[1.2.11 Remote Spoke 15](#_Toc36653435)

[1.2.12 Service Spokes 16](#_Toc36653436)

[1.2.13 Micro-Segmentation 16](#_Toc36653437)

[1.3 Network Considerations 18](#_Toc36653438)

[1.3.1 WAN and Azure Connectivity 18](#_Toc36653439)

[1.3.2 On-Premises Firewall Recommendations 18](#_Toc36653440)

[1.3.3 19](#_Toc36653441)

# Microsoft Azure

The customer requires an environment in Microsoft Azure that will be able to host current and future services that cannot be deployed using Software-as-a-Service (SaaS) offerings. This section of the high-level design will discuss that Azure deployment.

## Requirements

The below requirements are understood and accounted for in the design.

* **Migration**: Services will be migrated from DGI to Microsoft Azure. The Azure “Landing Zone” must offer a place to host these services and make then available to clients and for integration with other services.
* **Data centre exit**: A landing zone must be ready for migration to start by mid-Q3 2020. The old hosting environment should be vacated by 31/12/2021.
* **Future Innovation**: The customer has a strategic objective of embracing new technologies to create innovative and more efficient services for the municipality.
* **Migrated services**: The goal is that migrated services should be re-deployed in this preferential order: SaaS, PaaS, IaaS. The Landing Zone should allow for this or a mixture of deployment types.
* **Landing Zone properties**: The Azure Landing Zone should be new, modern, flexible, secure, and agile.
* **Landing Zone features**: The Landing Zone should have access control, access audit, logging, performance monitoring, encryption, automation, and backup.
* **Reduction in capital expenses**: Maximise the conversion of capital expenditure to operational expenditure.
* **Reduction of disruptions and improvement of IT stability**: The Azure deployment should reduce future migrations due to equipment obsolescence and improve the uptime of provided services.
* **Reduction in vendor or technical complexity**: Reducing the number of vendors and infrastructure/service complexity should be an objective of this design.
* **Optimization of internal operations**: Internal operations should be made quicker and easier.
* **Increase in business agility:** The environment should enable agile changes to existing services and the rapid introduction of new services.
* **Improved customer experiences and engagements**: A result of the migration and transformation of services with new agile methodologies should result in improved service delivery to internal customers and the municipality.

## Azure High-Level Design

### The Virtual Data Center

It is proposed that the Virtual Data Center (VDC) will be deployed as the Azure Landing Zone for the customer; this architecture is proven already in customer environments and is designed for governance, scale, agility, flexibility, and security.

### Terminology

The following terms are used in this section:

* **Tenant**: Based on an Azure Active Directory domain, the tenant is an organisation’s representation in a Microsoft cloud. A tenant can be used with one or many Microsoft clouds, such as Microsoft 365, Microsoft Azure, and CRM 365.
* **Subscription**: In the context of Microsoft Azure, a subscription is a logical boundary for cost management and role-based access control (RBAC). An Azure tenant might have one, a few, or many subscriptions. There is no cost to creating or owning a subscription – costs are created by resource usage, and the cost remains the same where resources are in one or many subscriptions.
* **Hub**: A hub is a central virtual network that mimics the functionality of a network core in a physical network deployment. The hub typically contains network resources that are used by many services, such as a virtual network gateway or a firewall.
* **Spoke**: A spoke is comparable to a VLAN or virtual network in an on-premises network. In the context of the VDC, a spoke is a subscription that contains a single service, whether it is using an Azure virtual network or not.

### VDC Concepts

The following are considerations in the design of the VDC:

* **Organization**: An organization will have a single governance, management, and security pane for centralized control of all deployed services. The organization may have one or more virtual data centre instances.
* **Region**: A VDC, like a physical data center, is associated with a physical location. All resources of a VDC, except for Azure global resources such as Traffic Manager, are deployed in a single region. For example, if a VDC is deployed into West Europe, then everything in that VDC is deployed into West Europe. If a VDC reaches the maximum number of possible spokes (495 based on /25 IPv4 spokes) then additional VDCs can be deployed in the same region. If an organization requires additional locations, either for distributed placement of resources or for disaster recovery, then additional VDCs can be deployed.
* **Enable Controlled DevOps**: The Governed VDC enables self-service with the guardrails of governance and security. The people that know security continue to implement security in the hub. Governance controls what is deployed. However, developers and operators are free to work within the loose constraints provided by the organization.
* **Isolation by Default**: An individual instance of a VDC does not trust anything outside of the VDC. It does not trust The Internet, other VDCs owned by the organization, or even the organization's on-premises networks. The VDC design isolates neighbouring spokes inside the same VDC. The goal is to prevent the spread of any attack or malware and to limit access by authorized staff at the network layer.
* **Connections**: The only public IP addresses allowed are in the hub of a VDC, unless there is a specific requirement from for a resource type by Microsoft Azure. This means that all data flows will pass through the hub - with some Microsoft-documented exceptions for the control plane of Azure platform services. All flows between spokes of the same VDC will pass through the hub of a VDC - no spoke should be peered with another spoke. Two VDCs owned by the same organization can be connected only via their hubs; ExpressRoute, VNet peering at the Network Hub, or Azure WAN any-to-any connectivity.
* **Resilience**: The VDC design does not rely on anything outside of the VDC. If authentication/authorization services are required, those services are deployed in and consumed from inside of the VDC. If administrative operations require a remote desktop connection to a VDC, the remote desktop connection is provided by components of the VDC, not by services from another VDC. The goal is that the VDC will continue to operate despite failures that may happen in on-premises networks or in other VDC deployments.
* **High Availability**: The services of a VDC are mission critical. For example, a virtual network gateway provides a secure connection between on-premises networks and the VDC. A firewall provides connectivity to spoke services. A web application firewall provides secure sharing of HTTP/S applications. Domain controllers provide DNS and authentication/authorization services to the network. Each of these components is deployed in a way to maximize the service level agreement (SLA) and the actual availability of the services. For example, if a VDC's Azure region supports Availability Zones, the zone redundancy is used with network resources and virtual machines are deployed across different zones. If a VDC's Azure region does not support Availability Zones, then virtual machines are deployed with Availability Sets.
* **Subscriptions**: Each service will be deployed into its own subscription and spoke. For example, if a new n-tier application with web, application, and database is being deployed, this service will be deployed into a single spoke/subscription. This approach simplifies support, cost-management, and role-based access control.
* **Edge Data Center (EDC)**: Sometimes, there will be a need to deploy a specific service outside of a VDC. For example, a VDC is placed in a small Azure region that does not support some required resource types or the nature of the service contradicts the design concepts of a VDC. In this case, the management & governance design provides the concept of an Edge Data Center (EDC), a service deployment that sits outside of a VDC but still under the same oversight and control.
* **PaaS and IaaS**: A VDC is not just for virtual machines. Admittedly, a lot of the conversation will be about networking, but most of the architecture of a VDC is designed to provide governance, security, and management for any kind of deployment in Microsoft Azure. A service does not need to be connected to a network to be a part of the governance and security architecture.
* **Subscriptions**: Azure subscriptions are used as a logical boundary for cost management, role-based access control, and support in the VDC. This means that there is one subscription per service. The core VDC is made up of 8 subscriptions. Each service added to that VDC (test, development, or production) will have its own subscription. This method simplifies the support experience and means that we can use the natural features of Azure for RBAC and cost management without any additional tooling.

### Infrastructure-as-Code (IaC)

The VDC is developed and deployed using Azure Resource Manager (ARM) JSON (JavaScript Object Notation) templates. has developed a library of modular templates. Each template takes several parameters (instructions or specialisations) to deploy a type of resource in Microsoft Azure, as well as configuring that resource and creating any necessary supporting resources. For example, the virtual machine template includes:

* The ability to deploy types/versions of Linux or Windows Server
* Configures diagnostics, monitoring & management
* Associates a backup schedule
* And more

An imprint provides a master design of the VDC. This imprint:

* Executes tasks to configure the Azure tenant/subscriptions
* Calls in necessary ARM templates from the IaC library
* Supplies parameters to configure individual resources that are created from the ARM templates

The IaC library and the imprint are stored in Azure DevOps. A pipeline provides continuous integration/continuous deployment (CI/CD) to the customer Azure tenant; this means that the imprint can be deployed to subscriptions in the customer’s Azure tenant, and changes can be made to the imprint to incrementally change the deployment over time. The connection between the DevOps subscription and the customer tenant is authenticated/authorized by an Azure Application (“SPN”) in the customer Azure Active Directory/tenant and can be severed by the customer at any time.

The customer will be given a copy of the IaC library and the imprint at the end of the deployment.

The pipeline is dealt with in different ways at the end of the deployment, depending on the nature of the engagement:

* Severed if the customer has no interest in maintaining a managed-services relationship with or in using Azure DevOps.
* Moved to a customer Azure DevOps subscription where the customer’s copy of the IaC library and imprint can be located, enabling the customer to continue to manage the VDC using CI/CD.
* Kept in place if the customer wishes to provide a managed service for the VDC.

### Governance

Azure has multiple services and tools that work together to provide complete management for not only applications running in Azure but also in other clouds and on-premises.

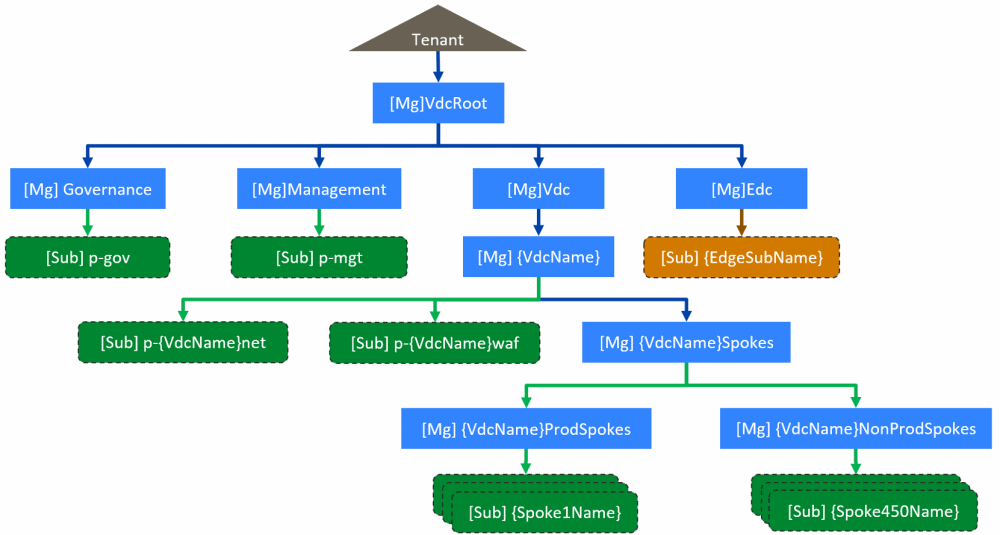


The VDC implements governance of all Azure resources from a centrally located subscription. Resources in this subscription and features of Microsoft Azure and Microsoft Azure Active Directory provide governance services:

* Management Groups: A hierarchical structure for organizing Azure subscriptions that is an inheritance-based model for deploying Azure Policy and Role-Based Access Control.
* Azure Policy: A process of deploying desired or mandatory configurations to audit or enforce organizational or regulatory compliance.
* Role-Based Access Control: The process of enabling access to systems with just-enough permissions to accomplish required tasks.
* Auditing: Recording and querying audit data of actions performed to resources by administrators, developers, operators, and Microsoft Azure.
* Resource Groups: Logical container within the subscription that is used to group all the manageable items required for a solution.
* Resource Locks: Locks applied on resources in order to protect them from accidental changes or deletion.
* Documentation Website: The website that this documentation is hosted on.
* Concierge: An product that delivers automated functionality to the VDC.

#### Management Groups

Management groups are created in a Microsoft tenant to organise Azure subscriptions. The hierarchy of management groups should reflect the administrative model of the Azure deployment. The following architecture is used in the VDC:



The management group hierarchy is used for:

* **Role-Based Access Control for Administrative Functions**: Custom roles are created in the tenant for Azure administration to grant specific granular rights. These roles are assigned to groups that are created for each management group in the hierarchy. Azure administrators are joined to the appropriate groups to grant them central rights over any subset hierarchy and any contained Azure subscriptions. Note the developer/operator rights are typically granted at the subscription level.
* **Azure Policy**: Policies can be assigned to management groups and their effects are inherited to the child subset of the hierarchy and contained Azure subscriptions.

Note that:

* Functions for governance and management are centralised and separated from service deployments.
* The design supports deploying many VDC instances in one or many Azure regions.
* The is flexibility for services that don’t fit the VDC construct or specific region(s) but should remain in the governance and security scaffold in the Edge Data Centre (EDC) management group.

#### Naming Standard

Many organisations have invested lots of time and effort into creating and maintaining a naming standard for on-premises resources. However, this naming standard will fail to handle the scales of Microsoft Azure:

* The many types of resources
* The quantity of resources with a single type/name
* The implicit relationships between resources

The VDC comes with a pre-built naming standard with the following properties:

* A prefix denotes the grade of service that is deployed, for example, production, test, or development.
* A code for the service identifies the service.
* Every subscription is named after the service and its deployment grade.
* Every resource group is named after the subscription that it is in and the specific function contained within the resource group.
* Any relationships between resources are constructed into the names of supporting resources.

When the IaC is used, the code will automate the naming of resources to respect the naming standard.

#### Azure Policy

An important function of governance is ensuring that IT implements desirable behaviour and configurations for the organisation; this includes respecting the security design of the environment. Azure Policy provides an ability to:

* Audit for undesired configurations and resource usage.
* Enforce desired configurations.
* Block undesirable resources or configurations.

The VDC includes a library of policies that can be assigned throughout the management group hierarchy and subscriptions to enforce governance and security design.

#### Role-Based Access Control (RBAC)

Administrators, developers and operators should have only enough access:

* To reach the resources the need for their roles/projects.
* Rights to do what needs to be done for the roles/projects.

A structured and manageable approach for RBAC in Azure is to:

* Create custom roles to create tasks with limited access/rights for different tasks.
* Create Azure AD groups for each management group and subscription.
* Assign roles to each to those groups.
* Add necessary user accounts to the appropriate groups to specify access rights and the scope of access.

Optionally, a feature of Azure Active Directory Premium called Privileged Identity Management (PIM) can be deployed to use just-in-time rights assignment for administrators, developers, and operators. PIM limits the rights that any one person has, and escalated rights on demand, with an optional approval process. PIM is not a standard component of the VDC deployment.

#### Auditing

Audit trails are created in two locations:

* **The tenant**: Azure AD creates an audit history of user/group actions and sign-ins (Azure AD Premium).
* **Azure subscriptions**: Each subscription maintains a 90-day history of a resource actions, by humans or by Azure.

These two sources of data are exported, just after creation, to two destinations:

* A dedicated storage account in the governance subscription. Here the data can be kept for many years. Data is kept in a read-only state. Each hourly log file is tiered to more cost-effective tiers of storage to facilitate long-term storage.
* A central log analytics workspace in a management subscription. The log data is kept for 1 year in a relational database, where it can be queried, visualised using Azure workbooks, and accessed/presented using Power BI.

#### Documentation Website

Every data centre should have an operations manual. The VDC contains documentation on:

* Governance
* The architecture of the environment
* The technical details of each VDC instance
* Procedures

The content is written in Markdown and typically shared with the customer in HTML format, shared on a dedicated storage account in the Governance subscription as a website.

### Management

A central subscription, called Management, hosts two resources to manage all VDC instances.

#### Log Analytics Workspace

A log analytics workspace (also referred to as a workspace or Azure monitor logs) is a relational database that stores monitoring, diagnostics, security, and performance metrics. A workspace uses Kusto Query Language (KQL) to query the data; these queries can be used to inspect data, or indirectly via Azure workbooks to visualise data in the Azure Portal. Power BI can be used to present visualisations outside of the Azure Portal, for example on a desktop, in SharePoint or in Microsoft Teams.

A central workspace is created in the Management subscription. This workspace receives all forms of monitoring from all Azure resources in the environment.

Access to this workspace is limited to those who have access to the Management subscription – this should be a few central IT administrators. Developers and operators who have access to Azure resources can query and view their own resources’ data through Azure Monitor or their resources in the Azure Portal.

The Workspace will retain 1 year of data – 1-year old data is automatically purged.

Microsoft Azure is increasingly adding Workbooks to take advantage of data stored in a workspace and it has become the strategic place for logging data from all resources. The VDC includes a set of:

* Saved KQL queries that are useful for diagnosing and troubleshooting networking issues.
* Azure workbooks for visualising data in key scenarios.

#### Azure Automation

An Azure automation account is deployed in the Management subscription to provide central configuration management services for virtual machines in all VDC instances. To enable the following tasks, the automation account is linked to the Management workspace for data storage/processing:

* **Update Management**: Patch deployment to the guest OS of Linux and Windows virtual machines.
* **Inventory & Change Tracking**: Creating an inventory of the guest OS of Linux/Windows virtual machines, and tracking changes to key items in those virtual machines.

### Security Management

Two security management systems are deployed in the VDC.

#### Azure Security Center

Azure Security Center is a security posture management system in Microsoft Azure. There are two tiers:

* **Basic Tier**: Available and active in all Azure subscriptions, Security Center will monitor resources and their configurations and make recommended security configuration changes. This data is also used to track compliance of several well-known security standards such as PCI-DSS and CIS. *Note: Security Center recommendations are not official guidance from Microsoft; they are generic scan/report audit policies that make some valuable recommendations and some recommendation that either do not understand the security design or will break basic functionality.* Recommendations should be viewed as a checklist of things that should be investigated, not as a set of instructed changes.
* **Standard Tier**: The paid-for Standard Tier provides additional functionality, including live monitoring of security signals from around the subscription, security alerts from Microsoft for your subscriptions/resources, and additional features such as threat detections for Azure SQL and storage accounts, and whitelisting of executables inside of a virtual machine guest OS. The Standard Tier is enabled in the hub subscriptions (the “network core”) of the VDC. It is recommended that the Standard tier is also enabled in subscriptions that contain sensitive services/data.

#### Azure Sentinel

Azure Sentinel is Microsoft’s cloud-based security information & event management (SIEM) service. Azure Sentinel offers:

* **Workspace integration**: Azure Sentinel will consume security data that is already being collected by a workspace.
* **Data collection**: The ability to collect security data from [other sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources), including Office 365, AWS, and third-party appliances.
* **Workbooks**: Several solutions visualise security data and trends.
* **Threat Hunting**: A customisable set of programmed tasks that can be executed as a response, scheduled, or started manually, will scan an environment looking for known threats or vulnerabilities.
* **Automated responses**: The quantity of security alerts can be overwhelming. Customisable playbooks can be triggered in the event of security alerts; this functionality is based on Azure logic apps, as is Microsoft Flow.

All available data sources are configured as part of the VDC deployment.

### Edge Data Centre (EDC)

The VDC environment provides flexibility to deploy services that might not fit into a VDC instance, either for configuration or location reasons.

A service can be deployed in an “edge data center” or EDC, a dedicated subscription that is placed in the EDC management group. This means that the service can still exist in the same governance, security, and management scaffold as VDC-based services but with a bit more flexibility.

### VDC Instance Design

The following is the network structure of a VDC instance:



The elements, each of which is a dedicated subscription, of this design are described below.

#### The Network Hub

Each VDC instance has its own Network Hub. There are three components to the Network Hub:

* **The Virtual Network**: The VNet provides network connectivity for the resources in the Network Hub, and to other internal and external services via site-to-site networking or VNet peering.
* **Virtual Network Gateway**: The function of the VNet gateway is to enable private connectivity to on-premises networks via site-to-site VPN and/or ExpressRoute. An alternative is to replace the VNet gateway with an Azure WAN hub for a software-defined WAN (SD-WAN).
* **Azure Firewall**: The Azure Firewall, which blocks everything (north-south and east-west) by default, provides a platform-based, DevOps-friendly, firewall for filtering traffic between outside the VDC and inside the VDC, and between spokes (services) inside the VDC. The entire configuration, including the rules collections, are configured using JSON and can be managed, with change control/approval/rollback, via Azure DevOps.

The purposes of the Network Hub are:

* Provide secure site-to-site network connections with on-premises networks.
* Secure the entry and exit of traffic from/to Internet sources/destinations.
* Provide a forced secure route between services deployed in the VDC. The Azure Firewall will be the default connection between a source and destination in different services, effectively changing the entire VDC into a collection of secure zones.

Each resource is highly available; in regions such as West Europe, a zonal or multi-zone deployment is used to increase the SLA from Microsoft Azure.

#### The Application Hub

An application hub provides a secure way to share HTTP/S services to on-premises, external, and VDC-based clients. The Azure web application firewall (WAF), which includes the application gateway Layer-7 load balancer, is used for this function. There are two WAFS in the design:

* **Private WAF**: Accessible only by Internal clients.
* **Public WAF**: Accessible only by Internet clients.

*Note: The Azure WAF cannot be used to share Citrix or Windows Virtual Desktop; they must be routed in a different way.*

Each WAF is deployed to a dedicated subnet in the Application hub with Layer-4 security provided by network security groups. Layer-7 (for example, SQL Injection attacks) inspection & filtering for HTTP/S traffic is provided by the OWASP 3.1 ruleset in the WAF. Layer-7 load balancing allows complex placement of HTTP/S services across many web servers/farms, and security optimisation such as SSL Offload and end-to-end encryption.

Version 2 of the Azure WAF is deployed for network flexibility and higher levels of availability, possible in regions such as West Europe. In addition, custom policy and managed is done using a WAF policy, and secrets (SSL certificates for offloaded SSL) are stored in Azure Key Vault with access to secrets being restricted to a minimum level using a managed user identity for the WAF instance.

Each WAF subnet is sized to allow:

* WAFs to scale out, either automatically or manually.
* Additional WAFs to be deployed.

### Domain Controllers Spoke

The first spoke, or service, deployed into the VDC is a pair of Active Directory Domain Services (ADDS) domain controllers (DCs). The address space of the VDC is defined as an ADDS site and is linked to any on-premises ADDS site for DC replication.

The function of the DCs in the VDC are:

* Provide authentication/authorisation for Windows Server-based services, such as Citrix or Windows Virtual Desktop.
* Offer name resolution services, particularly to resolve internal names, example, Azure API Management trying to connect to an API that is shared by the private WAF.

If these domain controllers are the only domain controllers in the entire organisation, they can be integrated with Azure AD for synchronisation.

Note: Azure AD Domain Services (AADDS) is not used in the VDC because:

* AADDS is only able to exist in a single Azure region and creates inflexibility and regional dependency issues.
* ADDS can exist without AAD, so it AAD has a local/global issue, authentication/authorisation and name resolution services in the VDC can still function.

Note: Azure Private DNS is not used because it is not compatible with all platform services.

The two DC virtual machines are deployed across availability zones for a higher SLA in regions such as West Europe, and in availability sets in other regions such as Norway East.

Security for the virtual machines is as follows:

* All traffic to/from the DC spoke must pass through the firewall in the Network Hub.
* All traffic to the DC spoke and inside the DC spoke must pass through a network security group firewall associated with the DC subnet.
* The disks of the DC virtual machines are encrypted, and the secret is stored in an Azure key vault virtual HSM.
* Automated patch management is provided by the central automation account.
* Windows Defender, managed with the Azure anti-malware extension, is deployed to secure the guest OS from the time of deployment.
* An Azure recovery services vault provides Azure Backup functionality to back up the virtual machines.

### Remote Spoke

The remote spoke is used to create an airgap between virtual machines hosted in the VDC and remote administrators/developers/operators.

A Remote Desktop Gateway (RDGW) cluster provides a secure reverse proxy to log into Windows Server virtual machines in the VDC. The Remote Desktop client connects to the RDGW cluster using HTPS, and upon successful login, the connection is relayed using RDP to the desired virtual machine.

One or more policies to configure access to VDC virtual machines are maintained on a pair of Network Policy Servers (NPS). Optionally, multi-factor authentication (MFA) can be enabled in some/all these policies with an integration with Azure AD Premium. With MFA enabled, the RDGW cluster can be securely shared on the Internet via a NAT rule in the Network Hub firewall.

A pair of Ubuntu Linux virtual machines provide SSH jump box functionality for Linux virtual machines. An administrator will log into one of these machines first, before logging into the desired Linux virtual machine in the VDC.

All the remote spoke virtual machines are deployed, as pairs, across availability zones for a higher SLA in regions such as West Europe, and in availability sets in other regions such as Norway East.

Security for the virtual machines is as follows:

* All traffic to/from the remote spoke must pass through the firewall in the Network Hub.
* All traffic to the remote spoke and inside the remote spoke must pass through a network security group firewall associated with the remote subnet.
* The disks of the remote virtual machines are encrypted, and the secret is stored in an Azure key vault virtual HSM.
* Automated patch management is provided by the central automation account.
* Windows Defender, managed with the Azure anti-malware extension, is deployed to secure the guest OS of the Windows virtual machines from the time of deployment.
* An Azure recovery services vault provides Azure Backup functionality to back up the virtual machines.

### Service Spokes

All services that are deployed in a VDC are deployed as dedicated subscriptions, whether they are network-joined, network-integrated or not:

Services that use a virtual network will be peered with both the Network Hub:

* The Network Hub firewall is used to route/secure inbound non-HTTPS traffic,
* All outbound traffic, except Azure control plane traffic, will exit the VDC through the firewall in the Network Hub.
* HTTP/S services will typically be shared via the WAFs in the Application Hub – note that an alternative is to share services with users using Azure AD Proxy for authentication/authorisation with multi-factor authentication (MFA).
* The service can access other HTTP/S services (in other spokes) via the private WAF in the Application Hub.

Services that do not use virtual networks can still be governed and secured by the scaffolding of the VDC.

Note that a single VDC instance can support up to 492 virtual network-enabled spokes where each spoke is deployed with a /25 virtual network. The Azure limit for a single hub is 500 spokes.

Spokes will not share operations/management features. For example:

* If a spoke requires Azure key vault for secret storage, it will have its own key vault.
* If a service requires Azure Backup, the spoke will have its own recovery services vault – centralised monitoring is available via Azure Monitor and the central workspace.
* If a service needs to execute runbooks, an azure automation account will be deployed in the spoke.

### Micro-Segmentation

The VDC is implemented using the network security concept of micro-segmentation. In this architecture, different forms of firewalls are implemented throughout the network and resource stack to restrict flows of traffic in all directions:

* Only traffic that is required by a service should be allowed into the service.
* The firewall in the Network Hub will control all egress traffic, to on-premises and to the Internet.

Multiple points of inspection exist for traffic entering a service. No service should trust any other service, effectively creating a network-based secure zone for every service.

Points of restriction include:

* The firewall in the Network Hub which does Layer-4 inspection & filtering on all inbound non-HTTPS traffic and all traffic leaving the VDC (on-premises or the Internet).
* The network security groups of the Application Hub WAFs restrict the traffic into the WAFs at Layer-4.
* The WAFs inspect requests for shared HTTP/S services at Layer-7, looking for things such as SQL injection attacks.
* Each subnet in a spoke virtual network has a network security group to provide additional Layer-4 filtering.
* Resources can also have forms of firewall protection:
  + Virtual machines have a guest OS firewall, which should remain operational.
  + Platform resources such as Azure SQL have a firewall to prevent unwanted connection attempts.
  + Other platform resources, such as App Services, have access rules to restrict who can be a client for their services.

Examples of flows are:

* **Inbound HTTPS request to App Service Standard**: The App Service is presented to clients using the public and/or private WAFs. A client resolves the custom domain name of the App Service and that resolves to the frontend IP address of the appropriate WAF. The browser attempts to connect to the frontend IP address of the WAF. Before the traffic reaches the WAF, the network security group for the WAF inspects/filters/logs the traffic at Layer-4. If the connection is allowed, the WAF receives the traffic where it is inspected/filtered/logged at Layer-7. If the application gateway configuration of the WAF shares the desired HTTP/S application, the connection will be relayed with the WAF now taking the role as client. A service endpoint in the WAF subnet will drop the web request to the App Service via the private Azure backbone (for better privacy and latency). The requests will reach the App Service where an access rule will check to see if the web request is originating from an approved WAF. If the requesting address is OK, the app service will respond to the WAF, which relays the response to the web client.
* **API Management Attempts to Resolve an Internal DNS Name**: API Management (APIM) is seeking an API server based on its fully qualified domain name (FQDN), which is hosted on an Active Directory Domain Services-integrated DNS. APIM uses the virtual network settings to determine the IP address of a DNS server – one of the VDC domain controller virtual machines. APIM sends a DNS request (connectionless UDP) to the domain controller via the firewall in the Network Hub. The firewall inspects/filters/logs the request attempt at Layer-4. If a rule allows the traffic, the DNS request is routed to the domain controller spoke. When the DNS request arrives in the subnet of the domain controller spoke, a network security group inspects/filters/logs the request at Layer-4. If the packet is allowed, it is copied into the NIC of the virtual machine where the guest OS firewall takes over. DNS is connectionless, so firewall rules must allow the response. The domain controller sends the response to the firewall in the Network Hub, which must allow the response. If allows, the response is routed to the virtual network in the APIM spoke, where the subnet network security group will also have to allow the response before it reaches APIM.

The above design provides isolation by default for services and the protection of data/assets:

* Every service is its own secure zone.
* Hackers face additional obstacles if they do penetrate a network.
* The reach of malware is extremely limited, unlike the typical wide-open on-premises VLAN that hosts many services.

Logging for the below firewalls is recorded:

* **Azure Firewall**: The Azure Firewall logs JSON logs to a storage account where it is retained for 3- days, enabling easy download and sharing. All data is also sent to the central Workspace for querying & visualisation and is also made available to Azure Sentinel.
* **Web application firewalls (WAFs)**: All logging data is sent to the central Workspace for querying & visualisation and is also made available to Azure Sentinel.
* **Network security groups (NSGs)**: NSG flow logs are sent to a storage account where they are retained for 30 days. That data is consumed every 10 minutes by the central Workspace where it is processed by the Network Watcher Traffic Analytics solution. Traffic Analytics classifies flows as normal or malicious, and identifies the source IP address, source country, and target IP address & port.

## Network Considerations

It has been agreed that this high-level design addresses a few networking topics.

### WAN and Azure Connectivity

The current state of the customer WAN is as follows:

* There are 45 locations around the municipality.
* Most locations are connected by a low latency dark fibre network with between 1 and 10 Gbps bandwidth.
* Some locations are connected using 4G. There is an ambition to leverage 5G.
* The town hall is the hub of WAN.

After some discussions with the customer, the following provisional plan has been proposed:

1. The customer shall continue to use the existing dark fibre and 4G network for the WAN.
2. An ExpressRoute circuit will be provisioned to connect the WAN with Microsoft Azure.
3. New network edge devices will be deployed by the customer; they should be compatible with Azure WAN.
4. The customer will migrate from dark fibre to an SD-WAN.
5. At this point, there will be more clarity about the need (by services) for and the performance traits of a site-to-site network connection to Microsoft Azure. The ExpressRoute circuit can be continued, replaced by an SD-WAN connection with Azure WAN hub, or opting to use encrypted public-only connections.

### On-Premises Firewall Recommendations

If an SD-WAN is in the future for the customer, enabling a mesh of VPN/ExpressRoute connections between sites & Microsoft Azure, would recommend one of the supported partners for Azure Virtual WAN that has listed documentation for configuration: <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-locations-partners#partners>.

There are two notable partners:

* Barracuda has done work on VPN tunnel/connection resilience.
* Citrix will offer optimisation for Citrix workloads running in Microsoft Azure.

Not listed, but due to be announced is a partnership between Cisco Meraki and Microsoft Virtual WAN. The advantage of Cisco Meraki is their strength in wireless networking.

HUB

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

A black screen with white lines

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with a black background

Description automatically generated with medium confidence

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A black screen with many lines

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with a black background

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

DNS

A black background with blue and white lines

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with a black line

Description automatically generated

Governance

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Policy on vdc root mgnt group

A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

IAC

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

VM workload

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with a black background

Description automatically generated with medium confidence

A black screen with white lines

Description automatically generated

A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Webapp workload

A black screen with white text

Description automatically generated

A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated