**Azure Landing Zone LLD**

**for**



**Author:**  Kyndryl

**Version:** Version 0.1

**Date:** Dec 2022

**Status**: Draft

**CONTENTS**

[1. Introduction 6](#_Toc125191122)

[1.1. Purpose 6](#_Toc125191123)

[1.2. Audience 6](#_Toc125191124)

[1.3. Scope 6](#_Toc125191125)

[1.4. Design considerations 6](#_Toc125191126)

[1.5. Related documents 7](#_Toc125191127)

[2. Requirements 8](#_Toc125191128)

[2.1. Functional requirements 8](#_Toc125191129)

[2.2. Non-functional requirements 9](#_Toc125191130)

[2.3. Risks, assumptions, issues, and dependencies 10](#_Toc125191131)

[3. Service design 11](#_Toc125191132)

[3.1. Architectural overview 11](#_Toc125191133)

[3.2. Service context 12](#_Toc125191134)

[3.3. Service components 13](#_Toc125191135)

[3.4. Service technologies 13](#_Toc125191136)

[3.5. Resource organization 14](#_Toc125191137)

[3.5.1. Naming convention 14](#_Toc125191138)

[3.5.2. Azure regions 15](#_Toc125191139)

[3.5.3. Management groups 15](#_Toc125191140)

[3.5.4. Subscriptions 16](#_Toc125191141)

[3.5.5. Resource groups 17](#_Toc125191142)

[3.5.6. Policies 21](#_Toc125191143)

[3.5.7. Resource tagging 22](#_Toc125191144)

[3.6. Identity and access management 23](#_Toc125191145)

[3.6.1. Corporate identity synchronization 23](#_Toc125191146)

[3.6.2. Authentication and authorization services/features 23](#_Toc125191147)

[3.6.3. Emergency access accounts 23](#_Toc125191148)

[3.6.4. Monitoring, logging, and alerting 23](#_Toc125191149)

[3.6.5. External users 23](#_Toc125191150)

[3.6.6. Access to resources 23](#_Toc125191151)

[3.7. Network topology and connectivity 24](#_Toc125191152)

[3.7.1. Virtual networks 24](#_Toc125191153)

[3.7.2. Network topology 25](#_Toc125191154)

[3.7.3. IP addressing 27](#_Toc125191155)

[3.7.4. Connectivity to Azure PaaS services 27](#_Toc125191156)

[3.7.5. Connectivity from/to the internet 27](#_Toc125191157)

[3.7.6. Traffic protection 28](#_Toc125191158)

[3.7.7. DNS name resolution 28](#_Toc125191159)

[3.8. Regulatory standards 28](#_Toc125191160)

[3.9. Security standard 29](#_Toc125191161)

[3.10. Platform automation and DevOps 30](#_Toc125191162)

[4. 31](#_Toc125191163)

[5. Abbreviations and definitions 31](#_Toc125191164)

List of changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Author(s) |
| 0.1 | 01-12-2022 | Initial version | Wojciech Pazdzierkiewicz, Kyndryl |
|  |  |  |  |

Document release

|  |  |  |
| --- | --- | --- |
| Role | Name | Date |
| Author | Kyndryl | Dec 2022 |
| Reviewer | Kyndryl | Dec 2022 |
| Reviewer | Dufry | Dec 2022 |
| Platform Lead | B. Bislimi |  |
| Cloud Architect | W. Pazdzierkiewicz |  |
| Target Audience | Platform Operations |  |

1. Introduction
   1. Purpose

The purpose of this document is to provide detailed design and architectural guidance required to implement an application centric Azure landing zones in accordance with Dufry delivery standards and portfolio services.

The mission is to create a cost-effective, application owner attractive and flexible management platform on Azure for application workloads. It must be ready to utilize various components and architectures based on application requirements, industry standards, vendor recommendations and operation capabilities.

* 1. Audience

This document is intended to cloud architects, designers and specialists tasked for provisioning and configuring the required Azure infrastructure, services and resources needed to implement the solution described in application architecture document.

* 1. Scope

The scope of Azure Landing Zone Solution Design covers the following:

* Architecture of Azure landing zones covering management groups, subscriptions, resource groups and resources layouts
* Network topology of Azure landing zones
* Policies for Azure based workloads
* Governance and compliance of the Azure landing zones including identity and access management and security baseline
* Cost management process
* Operational model including monitoring, service management, patching, updates, business continuity and platform automation

The following areas are explicitly out of scope:

* Management and maintenance of non-native Azure services and resources
* SaaS integrations
* GDC integration
  1. Design considerations

The following principles will apply to the creation of Azure landing zone:

* Landscape will be limited to consuming resources in four (4) regions:
  + West Europe (primary)
  + East US
  + Brazil South
  + North Europe

and other locations will be included in the later stage if any.

* PCI complaint workloads and segregation between production and non-production environments are delivered in isolated environments.
* Boundary between production and non-production environments is delivered on subscription level
* Application landing zones have been isolated each other on resource and communication level over network layer
* Application landing zones are delivered in dedicated spoke virtual networks as a part of global hub-spoke network topology
* UDRs are routed through firewall only between environments. Within one environment all subnets are routed locally
  1. Related documents

Several vendor best practice documentations have been used in this blueprint.

|  |  |
| --- | --- |
| Vendor | Document Name |
| Microsoft | Microsoft Cloud Adoption Framework for Azure  <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework> |
| Microsoft | Microsoft Azure Well-Architected Framework  <https://learn.microsoft.com/en-us/azure/architecture/framework/> |
| Microsoft | Terraform on Azure documentation  <https://learn.microsoft.com/en-us/azure/developer/terraform/> |
| Microsoft | Abbreviation examples for Azure resources  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations |
| Dufry | HLD Azure Landing zone design document  [Dufry Azure Landing zone design document\_v5.1.docx](https://dufry0.sharepoint.com/sites/DufryHybridCloud/Shared%20Documents/General/04%20RFP%20Due%20Diligence/Azure%20Landing%20Zone%20Design%20Workshop/Dufry%20Azure%20Landing%20zone%20design%20document_v5.1.docx?d=w0e040262b07143df9597535b6ec47354&csf=1&web=1&e=NfvBzd) |
| Dufry | Cost management discipline  [cost-management-discipline-template.docx](https://dufry0.sharepoint.com/:w:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Financial%20Control/cost-management-discipline-template.docx?d=w99e2dc233d6749cab67e14be7d119833&csf=1&web=1&e=LvSry9) |
| Dufry | Infrastrucure DevOps maturity  [Infrastructure DevOps Maturity](https://dufry0.sharepoint.com/:f:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Infrastructure%20DevOps%20Maturity?csf=1&web=1&e=e8fZaE) |

1. Requirements
   1. Functional requirements

|  |  |  |
| --- | --- | --- |
| Id | Category | Description |
| FR-01 | General standard | Tenant provides isolated development, test, and production environments |
| FR-02 | General standard | Tenant hosts approved application design patterns only |
| FR-03 | General standard | An application team receives read-only access to an application related production resource groups |
| FR-04 | General standard | An application team receives read-write access to an application related non-production resource groups |
| FR-05 | Network | All workloads are compartmentalized and isolated at the network level to meet security and operational best practices. |
| FR-06 | Network | Regional hub virtual networks ensure consistent and secure ingress/egress to the application hosting spoke virtual networks |
| FR-07 | Network | Spoke virtual networks provide logical network separation of workload by lifecycle phase, like development, tests, and production |
| FR-08 | Network | All workloads required corporate network connectivity run in a spoke virtual network |
| FR-09 | Network | All communication between spoke virtual networks is routed through the regional hub virtual network and appropriate network virtual appliance |
| FR-10 | Network | Spoke virtual networks are not peered with each other |
| FR-11 | Network | All network flows leverage secure communication protocols from source to target |
| FR-12 | Network | All network flows are managed using at least access pattern and are restricted to the only required ports/protocols |
| FR-13 | Network | All region-to-region communication flows through the regional hub virtual networks |
| FR-14 | Network | All workloads are deployed in an Azure region that has implemented the strategic hub-and-spoke architecture |
| FR-15 | Network | Production and non-production workloads run in separate spoke virtual networks without any communication between the workload types |
| FR-16 | Network | Dufry manages all the base network components, including but not limited to network security, virtual networks and IP address spaces, frontend network load-balancers, global traffic routing, etc. |
| FR-17 | Network | Each regional hub virtual network hosts core infrastructure that provides security services such as network scanning and log collection |
| FR-18 | IAM | Tenant IdP coincides with the company's primary Azure Active Directory |
| FR-19 | IAM | Users are configured with role-based access control using a least privilege model. Corporate Identity and Asset Management (IAM) standards enforce that users are only given permissions which are required for their job role |
| FR-20 | IAM | All requirements from this Standard for IAM related corporate controls are applicable to the tenant User IDs and privileges |
| FR-21 | IAM | All resources are grouped into resources groups to limit the user’s privileges to the minimum needed |
| FR-22 | IAM | Azure AD access groups are created based upon pre-defined roles (such as IAM User, Administrators, Auditors, Developers, Read Only) which are used for access management based upon the principle of at least privilege |
| FR-23 | IAM | Privileges/permissions are not applied to individual users. They are always assigned to Azure AD access groups instead. |
| FR-24 | IAM | Privileges of Azure AD access group are limited to a specific resource group |
| FR-25 | Security | All components within the tenant adhere to a “zero trust” model (i.e., where nobody and nothing is trusted by default) and require authentication/authorization from all other components. All access to applications, logs, data, and so on must require authentication and authorization to prevent misuse or unauthorized access. |
| FR-26 | Automation | Infrastructure team uses a DevSecOps process to provision cloud-based resources |
| FR-27 | Automation | Applications team uses a DevSecOps process configure cloud-based resources |
| FR-28 | Automation | Only up-to-date and trusted third-party components are used |

* 1. Non-functional requirements

|  |  |  |
| --- | --- | --- |
| Id | Category | Description |
| NFR-01 | Asset management | Use only approved services |
| NFR-02 | Asset management | Use only approved applications in virtual machine |
| NFR-03 | Backup and recovery | Ensure regular automated backups |
| NFR-04 | Backup and recovery | Protect backup and recovery data |
| NFR-05 | Backup and recovery | Monitor backups |
| NFR-06 | Backup and recovery | Regularly test backup |
| NFR-07 | Data protection | Discover, classify, and label sensitive data |
| NFR-08 | Data protection | Encrypt sensitive data in transit |
| NFR-09 | Data protection | Enable data at rest encryption by default |
| NFR-10 | Data protection | Use a secure key management process |
| NFR-11 | Data protection | Use a secure certificate management process |
| NFR-12 | Data protection | Ensure security of key and certificate repository |
| NFR-13 | DevSecOps | Secure DevOps infrastructure |
| NFR-14 | DevSecOps | Integrate static/dynamic application security testing into DevOps pipeline |
| NFR-15 | DevSecOps | Enforce security of workload throughout DevOps lifecycle |
| NFR-16 | DevSecOps | Enable logging and monitoring in DevOps |
| NFR-17 | Endpoint security | Use Endpoint Detection and Response (EDR) |
| NFR-18 | Endpoint security | Use modern anti-malware software |
| NFR-19 | Endpoint security | Ensure anti-malware software and signatures are updated |
| NFR-20 | Governance and Strategy | Align organization roles, responsibilities, and accountabilities |
| NFR-21 | Governance and Strategy | Follow enterprise segmentation/separation of duties strategy |
| NFR-22 | Governance and Strategy | Follow data protection strategy |
| NFR-23 | Governance and Strategy | Follow network security strategy |
| NFR-24 | Governance and Strategy | Follow security posture management strategy |
| NFR-25 | Governance and Strategy | Follow identity and privileged access strategy |
| NFR-26 | Governance and Strategy | Follow logging, threat detection and incident response strategy |
| NFR-27 | Governance and Strategy | Follow backup and recovery strategy |
| NFR-28 | Governance and Strategy | Follow endpoint security strategy |
| NFR-29 | Governance and Strategy | Follow DevOps security strategy |
| NFR-30 | Identity Management | Use centralized identity and authentication system |
| NFR-31 | Identity Management | Protect identity and authentication systems |
| NFR-32 | Identity Management | Manage application identities securely and automatically |
| NFR-33 | Identity Management | Authenticate server and services |
| NFR-34 | Identity Management | Use strong authentication controls |
| NFR-35 | Identity Management | Restrict resource access based on conditions |
| NFR-36 | Identity Management | Restrict the exposure of credential and secrets |
| NFR-37 | Identity Management | Secure user access to existing applications |
| NFR-38 | Network Security | Establish network segmentation boundaries |
| NFR-39 | Network Security | Secure cloud services with network controls |
| NFR-40 | Network Security | Deploy intrusion detection/intrusion prevention systems (IDS/IPS) |
| NFR-41 | Network Security | Deploy DDOS protection |
| NFR-42 | Network Security | Deploy web application firewall |
| NFR-43 | Network Security | Simplify network security configuration |
| NFR-44 | Network Security | Detect and disable insecure services and protocols |
| NFR-45 | Network Security | Connect on-premises or cloud network privately |
| NFR-46 | Network Security | Ensure Domain Name System (DNS) security |
| NFR-47 | Privileged Access | Separate and limit highly privileged/administrative users |
| NFR-48 | Privileged Access | Avoid standing access for user accounts and permissions |
| NFR-49 | Privileged Access | Follow just enough administration (least privilege) principle |

* 1. Risks, assumptions, issues, and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref. | Type | Description | Owner | Action |
| A001 | Assumption |  | Kyndryl |  |
| A002 | Assumption |  | Dufry |  |
| A003 | Assumption |  | Kyndryl |  |
| A004 | Assumption |  | Kyndryl |  |
| D001 | Dependency |  | Kyndryl |  |

1. Service design
   1. Architectural overview

This section provides the architecture overview of the target design of landing zone concept for the applications to be hosted in Azure.

To facilitate the understand, there are defined certain terms as follows:

Tenant

According to Microsoft “a tenant is a group of users or an organization that share access with specific privileges to an instance of a product, service, or application. In Azure Active Directory a tenant is an instance of Azure Active Directory that an organization receives when it signs up for a cloud application like Microsoft 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants. Multitenancy refers to an instance of an application shared by multiple organizations, each with separate access to the instance.”

Dufy company uses “Dufry International AG” Azure organization tenant and has deployed resources in multiple subscriptions that are organized using management groups.

Management Platform

According to Microsoft “Management refers to the tasks and processes required to maintain your business applications and the resources that support them. Azure has many services and tools that work together to provide complete management. These services aren't only for resources in Azure, but also in other clouds and on-premises.”

The management comprises the areas of configuration, monitoring, security, protection, governance (e.g. cost management) and migration. The relevant tools and services are part of the management platform in the proposed tenant layout. The segregation of application landing zones establishes the necessary distinction in the RBAC and the relevant policies and permissions.

Landing Zones

The definition of a landing zone at Microsoft is as follows:

“An Azure landing zone is the output of a multi-subscription Azure environment that accounts for scale, security governance, networking, and identity. An Azure landing zone enables application migration, modernization, and innovation at enterprise-scale in Azure. This approach considers all platform resources that are required to support the customer's application portfolio and doesn't differentiate between infrastructure as a service or platform as a service.

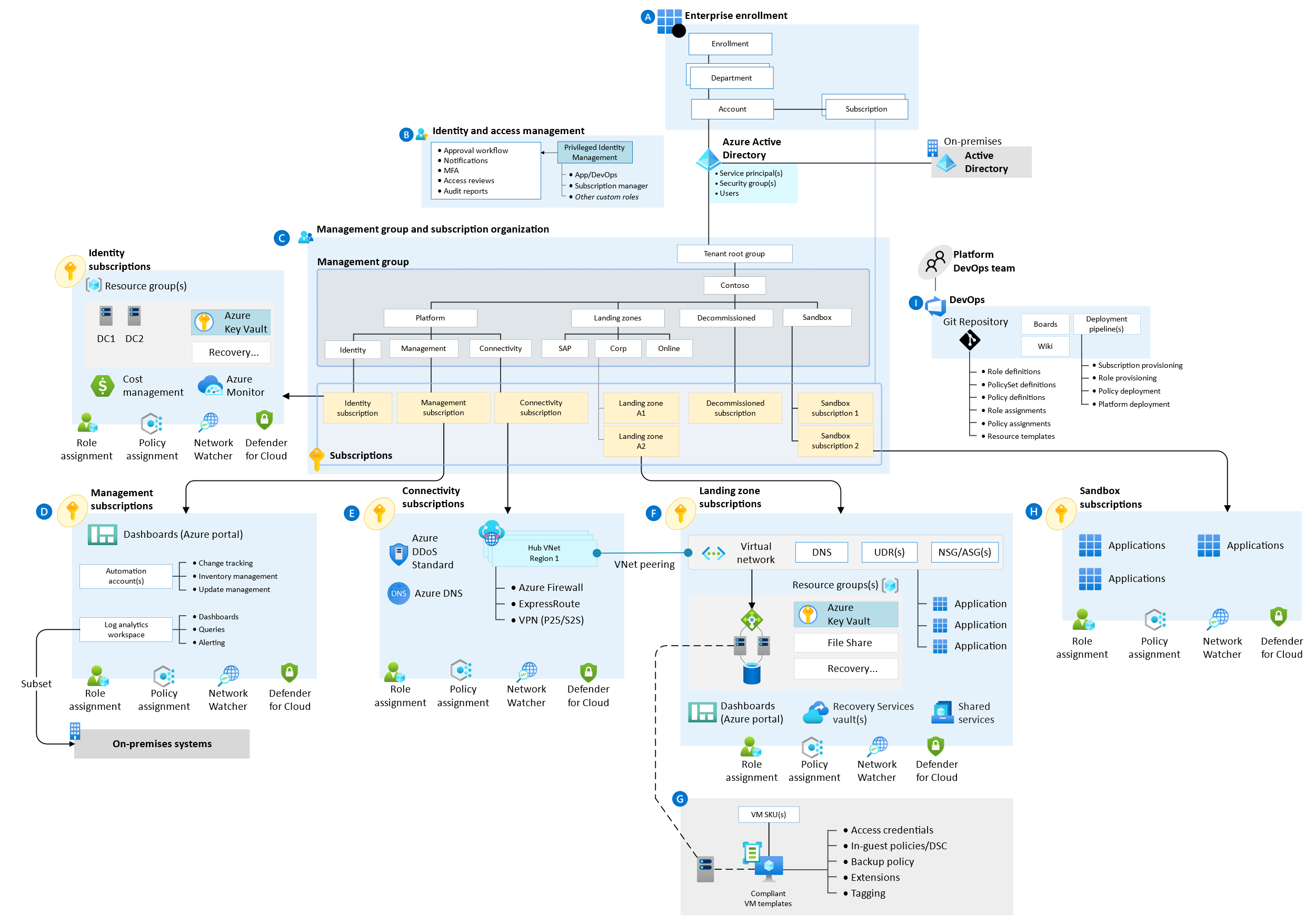
A landing zone is an environment for hosting your workloads, pre-provisioned through code.”

Dufry foreseeing various number of landing zones, for application workloads. The landing zones contain a test and a production environment.

* 1. Service context

Dufry intends to leverage Azure cloud services in its Digital Journey and enable transformation of services into cloud. In the initial scope Dufry Switzerland GDCs are considered for extension into Azure and scale for future requirements and other regions. This section describes in detail out various solution components and architecture of IaaS centric Azure landing zone.

The following architecture is used as a starting point. It is modified accordingly to the specific business and technical requirements when planning landing zone implementation for application workload.



Ref.: [What is an Azure landing zone? - Cloud Adoption Framework | Microsoft Learn](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/#azure-landing-zone-conceptual-architecture)

Ref. example of adoption: [POS API Manangement](https://dufry0.sharepoint.com/:f:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/POS%20API%20Manangement?csf=1&web=1&e=vfX8T7)

* 1. Service components

|  |  |
| --- | --- |
| Category | Service |
| Network | Virtual network |
| Private DNZ zone |
| Virtual network gateway: VPN |
| Network security group |
| Application security group |
| Network Watcher |
| Route tables |
| Application gateway |
| Load balancer |
| Compute | Virtual machine |
| Virtual machine scale set |
| Kubernetes services |
| Store | Blob storage |
| File storage |
| Key vault |
| Database | SQL servers |
| SQL databases |
| Security | Azure Active Directory |
| Azure AD Privilege Identity Management |
| Azure AD Conditional Access |
| Multifactor authentication |
| Identity Governance |
| Microsoft Defender for Cloud |
| General | Monitor |
| Policy |
| Alerts |
| Recovery Services vaults |
| Update management |
| Automation accounts |
| Log Analytics workspace |

* 1. Service technologies

This project is fully based in services and resources from the Infrastructure as a Service and Platform as a Service (PaaS) offering in Azure. All technologies are based on Azure services and Microsoft products on these.

* 1. Resource organization
     1. Naming convention

Dufry incorporates the following standard:

[Abbreviation examples for Azure resources - Cloud Adoption Framework | Microsoft Learn](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations)

with the modification:

|  |  |  |
| --- | --- | --- |
| Resource type | Pattern | Example |
| management group | <purpose> | <company identifier> | CORPAPPS  DUF  HUD |
| subscription | <company identifier>-<service identifier>-<environment>-<sequence> | duf-infra-001 hud-infra-001 duf-corpapps-001 |
| resource group | rg-<company identifier>-<Cloud Region>-<service identifier>-<purpose>-<environment> | rg-duf-weu-infra-hub-prod rg-duf-eus-infra-hub-prod rg-duf-sea-infra-hub-prod |
| virtual machine | [XX]<cloud identifier><server type><sequence number><environment> | AZUDUFAPP001LP  DEHAMSRV001P  XXAZUSRV001P |
| storage account | st-<company identifier>-<cloud region>-<service identifier>-<purpose>-<environment> | st-duf-shared-loganalytics-prod |
| virtual network | vnet-<company identifier>-<Cloud Region>-<service identifier> | vnet-duf-weu-infra vnet-hud-weu-infra vnet-duf-weu-corpapps |
| subnet | snet-<company identifier>-<Cloud Region>-<service identifier>-<purpose>-<environment>-<address space> | snet-duf-weu-infra-gateway-prod-10.25x.0.0/xx snet-duf-weu-corpapps-web-prod-10.25x.0.0/xx snet-duf-weu-corpapps-app-prod-10.25x.0.0/xx |
| virtual network peering | vnp-<company identifier>-<Cloud Region>-<service identifier> | vnp-duf-weu-infra-hub-prod  vnp-duf-weu-erp-app-prod  vnp-duf-weu-corpapps-prod |
| network security group | nsg-<company identifier>-<service identifier>-<purpose>-<environment> | nsg-duf-corpapps-app-prod nsg-duf-corpapps-database-prod nsg-duf-corpapps-web-prod |
| local network gateway | lgw-<company identifier>-<cloud region>-<service identifier> | lgw-duf-weu-infra |
| virtual network gateway | vgw-<company identifier>-<service identifier>-<purpose> | vgw-duf-weu-infra vgw-hud-eus-infra |
| virtual network gateway connection | vgwcn-<company identifier>-<cloud region>-<service identifier> | vgwcn-duf-weu-infra |
| Azure AD group | adg-<company identifier>-<service identifier>-<role>-<access level> | adg-duf-infra-contributor-sub adg-duf-infra-owner-rg adg-duf-corpapps-reader-sub |
| recovery service vault | rsv-<company identifier>-<Cloud Region>-<service identifier> | rsv-duf-weu-infra rsv-duf-sea-corpapps rsv-duf-neu-infra |
| backup policy | bup-<company identifier>-<Cloud Region>-<service identifier>-<purpose> | bkp-duf-weu-infra-vm bkp-duf-sea-corpapps-fs bkp-duf-neu-infra-db |
| log analytics workspace | law-<company identifier>-<Cloud Region>-<service identifier> | law-duf-weu-infra  law-duf-weu-erp law-duf-sea-corpapps |
| public IP address | pip-<company identifier>-<service identifier>-<purpose> | pip-duf-weu-infra-fw  pip-duf-weu-infra-vgw  pip-duf-weu-infra-bastion-prod |
| automation account | aac-<company identifier>-<cloud region>-<service identifier> | aac-duf-weu-infra  aac-duf-weu-erp  aac-duf-weu-corpapps |
| Azure monitoring alert | ar<company identifier>-<cloud region>-<service identifier>-<purpose> | ar-duf-corpapps-service-health-sub |
| Azure monitoring alert rule | malrt<company identifier>-<cloud region>-<service identifier>-<purpose> | malrt-duf-weu-infra-vm |
| Azure policy definition | pd-<company identifier>-<cloud region>-<service identifier>-<purpose> | pd-resourcegroup-tags-createdOnDate |
| Azure policy initiative | plcint-<company identifier>-<cloud region>-<service identifier>-<purpose> | plcint-duf-weu-infra-vm |

|  |
| --- |
| Business/company identifiers |
| DUF |
| TNG |
| HUD |
| WDF |

|  |
| --- |
| Service Identifiers |
| CORPAPPS |
| ERP |
| STORE SYSTEMS |
| INFRA |

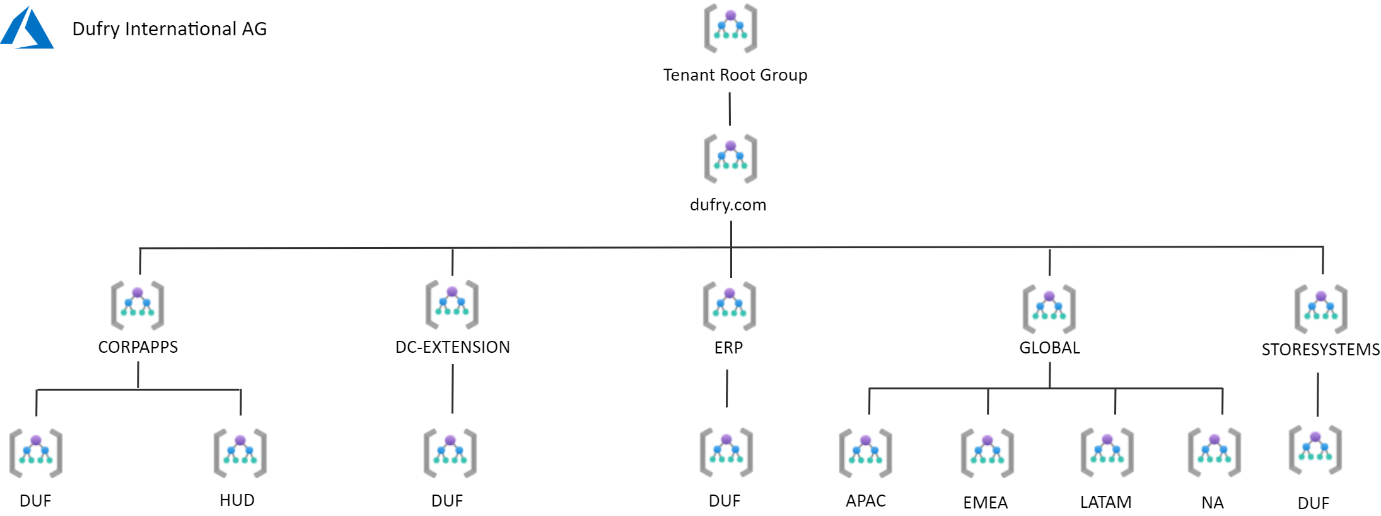
* + 1. Azure regions

Based on services offered and commercial aspects, the following regions are selected:

|  |  |  |
| --- | --- | --- |
| Location | No resources | Category |
| West Europe | 2116 | Primary |
| East US | 78 | Secondary |
| Brazil South | 4 | Secondary |
| North Europe | 1 | Secondary |
| Global | 34 | <build in> |

* + 1. Management groups

As azure management groups help to organize resources and subscriptions, including applying policies, RBAC and cost management, the following structure is used to meet business needs:



Ref.: [Dufry\_Azure\_Landing\_Zone\_LLD\_v0.1-MG.png](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ref/Dufry_Azure_Landing_Zone_LLD_v0.1-MG.png?csf=1&web=1&e=tGJbf5)

|  |  |  |
| --- | --- | --- |
| Management Group Id | Management Group Name | Purpose |
| <guid> | Tenant Root Group | <default> |
| dufry.com | dufry.com | This management group is located directly under the tenant root group. Created with a prefix provided by the organization, which purposely avoids the usage of the root group so that organizations can move existing Azure subscriptions into the hierarchy. It also enables future scenarios. |
| CORPAPPS | CORPAPPS | The parent management group for the corporate application landing zone child management groups. It has workload agnostic Azure policies assigned to ensure workloads are secure and compliant. |
| CORPAPPS > DUF | CORPAPPS > DUF | Main corporate application landing zone management group |
| CORPAPPS > HUD | CORPAPPS > HUD | Hudson corporate application landing zone management group |
| DC-EXTENSION | DC-EXTENSION | Parent GDC extension management group |
| DC-EXTENSION > DUF | DC-EXTENSION > DUF | The dedicated management group for restricted corporate landing zone. This group is for workloads that require connectivity or hybrid connectivity with the corporate network via the hub in the connectivity subscription. |
| ERP | ERP | Parent ERP management group |
| ERP > DUF | ERP > DUF | The dedicated management group for ERP landing zones |
| GLOBAL | GLOBAL | Parent regional management group |
| GLOBAL > APAC | GLOBAL > APAC | The dedicated management group for APAC workload |
| GLOBAL > EMEA | GLOBAL > EMEA | The dedicated management group for EMEA workload |
| GLOBAL > LATAM | GLOBAL > LATAM | The dedicated management group for LATAM workload |
| GLOBAL > NA | GLOBAL > NA | The dedicated management group for NA workload |
| STORESYSTEMS | STORESYSTEMS | Parent STORSYSTEMS management group |
| STORESYSTEMS > DUF | STORESYSTEMS > DUF | The dedicated management group for subscriptions that are only be used for storesystem applications like TPv4, TPv6, iTEK, etc. |

* + 1. Subscriptions

Subscriptions are a unit of management, billing, and scale within Azure. They play a critical role when you're designing for large-scale Azure adoption.

If the business requirements change over time, the architecture allows for creating additional subscriptions and placing them into the suitable management group and assigning Azure policies.

As Azure service presents a range of active subscription offers Dufry use Enterprise Agreement (Enterprise Agreement) Support.

Graphical user interface

Description automatically generated with medium confidence

Ref.: [Dufry\_Azure\_Landing\_Zone\_LLD\_v0.1-SUB.png](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ref/Dufry_Azure_Landing_Zone_LLD_v0.1-SUB.png?csf=1&web=1&e=v71SP1)

|  |  |  |
| --- | --- | --- |
| Subscription | No resources | Purpose |
| duf-br-corpapps-prod | 4 | Subscription that is only used for the production stage of corporate applications in LATAM |
| duf-corpapps-001 | 334 | Subscription that is only used for the production stage of corporate applications |
| duf-corpapps-non-prod | 268 | Subscription that is only used for the non-production stage of corporate applications |
| duf-erp-001 | 109 | Subscription that is only used for the production stage of ERP applications |
| duf-infra-001 | 605 | Dedicated subscription for connectivity. This subscription hosts the Azure networking resources required for the platform, like Azure Network Gateways, Azure Firewall, and Azure DNS private zones. |
| duf-security-non-prod | 51 | Subscription that is only used for security related applications like Splunk, Sailpoint, Cyberark, etc.in non-production stage |
| duf-security-prod | 229 | Subscription that is only used for security related applications like Splunk, Sailpoint, Cyberark, etc.in production stage |
| duf-storesystems-non-prod | 75 | Subscription that is only used for storesystems applications like TPv4, TPv6, iTEK, etc.in non-production stage |
| duf-storesystems-prod | 7 | Subscription that is only used for storesystems applications like TPv4, TPv6, iTEK, etc.in production stage |
| DUFRY DEV/TEST/POC | 369 | Subscription that is only used for education and exploration by an organization. This subscription will be securely disconnected from the other landing zones. |
| DUFRY Production | 17 | Legacy subscription that is used for various solutions, including ML, etc. |
| DUFRY SANDBOX | 1 | Subscription that is only used for development of applications. This subscription is securely disconnected from the other landing zones. |
| DUFRY\_MASTERDATA | 81 | Dedicated subscription that is only used for MASTERDATA application |
| Dufry-CloudReach | 0 | <n/a> |
| hud-corpapps-001 | 73 | Subscription that is only used for the production stage of Hudson corporate applications |
| Microsoft Azure Enterprise | 0 | <n/a> |

* + 1. Resource groups

Diagram

Description automatically generatedMultiple Azure resources are grouped together into below Azure resource groups with given, under various subscriptions

Ref.: [Dufry\_Azure\_Landing\_Zone\_LLD\_v0.1-RG.png](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ref/Dufry_Azure_Landing_Zone_LLD_v0.1-RG.png?csf=1&web=1&e=2Nhw6X)

|  |  |  |
| --- | --- | --- |
| Subscription | Resource group name | Purpose |

|  |  |  |
| --- | --- | --- |
| duf-br-corpapps-prod | rg-duf-sbr-corapps-storeapp-prod |  |
| duf-br-corpapps-prod | rg-duf-sbr-corapps-storeapp-qua |  |
| duf-corpapps-001 | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| duf-corpapps-001 | Case2206280050001264 |  |
| duf-corpapps-001 | cloud-shell-storage-westeurope |  |
| duf-corpapps-001 | DefaultResourceGroup-WEU |  |
| duf-corpapps-001 | NetworkWatcherRG |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-advandpromo-aks-nodes-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-advandpromo-aks-nodes-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-advandpromo-preprod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-advandpromo-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-assortmgmt-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-azurebackup1 |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-bec-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-bec-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-bec-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-concessions-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-concessions-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-concessions-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-aks-nodes-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-aks-nodes-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-aks-nodes-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-preprod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-dufryhub-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-infra |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-insights-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-integration-kafka-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-aks-nodes-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-aks-nodes-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-aks-nodes-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-dev |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-prod |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-pricepolicy-quality |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-sharedservices |  |
| duf-corpapps-001 | rg-duf-weu-corpapps-sipandshiftplan-prod |  |
| duf-corpapps-001 | VisualStudioOnline-C04D9CAE8FD244D5970B51283DD7C508 |  |
| duf-corpapps-non-prod | NetworkWatcherRG |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-advandpromo-aks-nodes-quality |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-advandpromo-quality |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-assortmgmt-dev |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-assortmgmt-preprod |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-backups-aks-non-prod |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-backups-non-prod |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-docandtraining-dev |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-infra-non-prod |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-insights-dev |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-insights-test |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-insights-uat |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-integration-kafka-dev |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-integration-kafka-dev-aks-nodes |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-integration-kafka-quality |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-integration-kafka-quality-aks-nodes |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-sharedservices-non-prod |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-sipandshiftplan-dev |  |
| duf-corpapps-non-prod | rg-duf-weu-corpapps-sipandshiftplan-quality |  |
| duf-erp-001 | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| duf-erp-001 | AzureBackupRG\_westeurope\_1 |  |
| duf-erp-001 | cloud-shell-storage-westeurope |  |
| duf-erp-001 | duf-weu-erp-centralfinance-netapp |  |
| duf-erp-001 | NetworkWatcherRG |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-dev |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-lb-prod |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-prod |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-quality |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-sandbox |  |
| duf-erp-001 | rg-duf-weu-erp-centralfinance-temp |  |
| duf-erp-001 | rg-duf-weu-erp-infra |  |
| duf-erp-001 | rg-duf-weu-erp-mgmt-prod |  |
| duf-infra-001 | AzureBackupRG\_westeurope\_1 |  |
| duf-infra-001 | cloud-shell-storage-westeurope |  |
| duf-infra-001 | dashboards |  |
| duf-infra-001 | DefaultResourceGroup-WEU |  |
| duf-infra-001 | LogAnalyticsDefaultResources |  |
| duf-infra-001 | NetworkWatcherRG |  |
| duf-infra-001 | rg-duf-weu-infra-adca-prod |  |
| duf-infra-001 | rg-duf-weu-infra-adconnect-prod |  |
| duf-infra-001 | rg-duf-weu-infra-app |  |
| duf-infra-001 | rg-duf-weu-infra-automation-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-external-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-img-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-insights-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-internal-apac-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-internal-emea-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-internal-nala-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-officeonline-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-sharedservices-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-tpnet-prod |  |
| duf-infra-001 | rg-duf-weu-infra-avd-ws-prod |  |
| duf-infra-001 | rg-duf-weu-infra-bastion-prod |  |
| duf-infra-001 | rg-duf-weu-infra-company-communicator-prod |  |
| duf-infra-001 | rg-duf-weu-infra-fw-ip-groups-prod |  |
| duf-infra-001 | rg-duf-weu-infra-hub-prod |  |
| duf-infra-001 | rg-duf-weu-infra-mon-non-prod |  |
| duf-infra-001 | rg-duf-weu-infra-mon-prod |  |
| duf-infra-001 | rg-duf-weu-infra-nerdio-prod |  |
| duf-infra-001 | rg-duf-weu-infra-sccm-reporting-prod |  |
| duf-infra-001 | rg-duf-weu-infra-sharedservices-non-prod |  |
| duf-infra-001 | rg-duf-weu-infra-sharedservices-prod |  |
| duf-infra-001 | rg-duf-weu-infra-solarwinds-prod |  |
| duf-infra-001 | rg-duf-weu-infra-wiki-prod |  |
| duf-infra-001 | rg-duf-weu-infra-wvd-prep-image-non-prod |  |
| duf-infra-001 | rg-duf-weu-infra-wvd-shared-prod |  |
| duf-infra-001 | rg-hud-weu-infra-adc-prod |  |
| duf-infra-001 | WVDAutoScaleResourceGroup |  |
| duf-infra-001 | XXAZUIMGRG001WP |  |
| duf-infra-001 | XXAZURGGMTWP |  |
| duf-infra-001 | XXAZURGHPWP |  |
| duf-infra-001 | XXAZUSTGRG001WP |  |
| DUFRY DEV/TEST/POC | dashboards |  |
| DUFRY DEV/TEST/POC | databricks-rg-rgdufryinsightsdatabricks-gciw7pbwzasi6 |  |
| DUFRY DEV/TEST/POC | NetworkWatcherRG |  |
| DUFRY DEV/TEST/POC | rg-duf-weu-corpapps-audins-poc |  |
| DUFRY DEV/TEST/POC | rg-duf-weu-corpapps-di-staging-test |  |
| DUFRY DEV/TEST/POC | rg-duf-weu-corpapps-dmpd-dev |  |
| DUFRY DEV/TEST/POC | rg-duf-weu-corpapps-insights-jeldebfin-dev |  |
| DUFRY DEV/TEST/POC | RG\_DUFRY\_CORPAPP\_DEV\_TEST\_POC |  |
| DUFRY DEV/TEST/POC | RG\_DUFRY\_CORPAPP\_KAFKA\_TEST\_POC |  |
| DUFRY DEV/TEST/POC | RG\_DUFRY\_FOUNDATION\_DEV\_TEST\_POC |  |
| DUFRY DEV/TEST/POC | RG\_DUFRY\_PHOENIX\_DEV\_TEST\_POC |  |
| DUFRY DEV/TEST/POC | RG\_RAPID\_INSIGHTS |  |
| DUFRY Production | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| DUFRY Production | NetworkWatcherRG |  |
| DUFRY Production | RG-AuditArchive |  |
| DUFRY Production | RG-MachineLearning-RubenPertusa-Lopez |  |
| DUFRY Production | RG\_DUFRY\_FOUNDATION\_PROD |  |
| DUFRY SANDBOX | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| DUFRY SANDBOX | NetworkWatcherRG |  |
| DUFRY\_MASTERDATA | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| DUFRY\_MASTERDATA | AzureBackupRG\_westeurope\_1 |  |
| DUFRY\_MASTERDATA | DefaultResourceGroup-WEU |  |
| DUFRY\_MASTERDATA | NetworkWatcherRG |  |
| DUFRY\_MASTERDATA | RG-DUF-MASTERDATA-PROD |  |
| DUFRY\_MASTERDATA | RG-DUF-MASTERDATA-SPLUNK |  |
| Dufry-CloudReach | cloud-shell-storage-northeurope |  |
| Dufry-CloudReach | cloudreach-monitoring |  |
| Dufry-CloudReach | NetworkWatcherRG |  |
| duf-security-non-prod | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| duf-security-non-prod | DefaultResourceGroup-WEU |  |
| duf-security-non-prod | NetworkWatcherRG |  |
| duf-security-non-prod | rg-duf-weu-security-infra-non-prod |  |
| duf-security-non-prod | rg-duf-weu-security-sailpoint-non-prod |  |
| duf-security-prod | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| duf-security-prod | AzureBackupRG\_westeurope\_1 |  |
| duf-security-prod | NetworkWatcherRG |  |
| duf-security-prod | rg-duf-weu-security-cortex-prod |  |
| duf-security-prod | rg-duf-weu-security-cyberark-prod |  |
| duf-security-prod | rg-duf-weu-security-cyberintelligencehub-prod |  |
| duf-security-prod | rg-duf-weu-security-eventhub-prod |  |
| duf-security-prod | rg-duf-weu-security-goanywhere-prod |  |
| duf-security-prod | rg-duf-weu-security-infra-prod |  |
| duf-security-prod | rg-duf-weu-security-sailpoint-prod |  |
| duf-security-prod | rg-duf-weu-security-sharedservices-prod |  |
| duf-security-prod | rg-duf-weu-security-splunk-prod |  |
| duf-security-prod | rg-duf-weu-security-tenablead-prod |  |
| duf-security-prod | rg-duf-weu-security-umbrella-prod |  |
| duf-storesystems-non-prod | rg-duf-weu-storesystems-apim-dev |  |
| duf-storesystems-non-prod | rg-duf-weu-storesystems-infra-non-prod |  |
| duf-storesystems-non-prod | rg-duf-weu-storesystems-itek-dev |  |
| duf-storesystems-non-prod | rg-duf-weu-storesystems-ombori-dev |  |
| duf-storesystems-non-prod | rg-duf-weu-storesystems-tpv6-dev |  |
| duf-storesystems-prod | rg-duf-weu-storesystems-infra-prod |  |
| hud-corpapps-001 | azureapp-auto-alerts-02a670-sashko\_jordanov\_dufry\_com |  |
| hud-corpapps-001 | dashboards |  |
| hud-corpapps-001 | DefaultResourceGroup-WEU |  |
| hud-corpapps-001 | NetworkWatcherRG |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-infra |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-aks-nodes-dev |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-aks-nodes-prod |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-aks-nodes-test |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-dev |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-prod |  |
| hud-corpapps-001 | rg-hud-eus-corpapps-masterdata-test |  |

* + 1. Policies

Graphical user interface

Description automatically generated with medium confidenceAzure Policy helps to enforce Dufry organizational standards and to assess compliance at-scale and evaluates resources and actions in Azure by comparing the properties of those resources to business rules known as policy definitions. Several of them are grouped together to form a policy initiative and is assigned to Dufry.com management group scope.

[duf-pol.PNG](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_inventory/duf-pol.PNG?csf=1&web=1&e=Hux9dO)

The following effects are used in Azure landing zones environment to control and audit subscriptions and their resources:

* Audit
* AuditIfNotExists
* Deny
* Modify

Graphical user interface, application

Description automatically generated

* + 1. Resource tagging

Information captured in tags is used for reaching out to right application contacts during major outage, charge back to respective cost center, authorizing right privileges etc.

Resource tagging is implemented on resource group level over 2 policies:

* “Mandatory Tags initiative for resource groups”, scoped to “dufry.com” management group to deny creation of resource groups without below tags
* “Global Tagging Policy”, scoped to “dufry.com” management group to inherits tags by resources from resource group ones

The following mandatory resource tags are implemented:

|  |  |  |
| --- | --- | --- |
| Key | Value | Purpose |
| Application Name | <application name> | Application/initiative description |
| Cost Center | <cost center> | Cost center number, like 4509 |
| DMZ | Yes | No |  |
| Data Classification | Internal | Confidential |  |
| Financial owner | <name of financial owner> |  |
| Global HFM Code | <global hfm code> |  |
| Hosting Environment | PROD | NON-PROD |  |
| Regulatory Compliance | PCI | GDP | PII |  |
| Service owner | <name of service owner> |  |
| Technical contact | <name of technical contact> |  |

The following optional resource tags are implemented:

|  |  |  |
| --- | --- | --- |
| Key | Value | Purpose |
| Hosting Region | East US | West Europe |  |
| Hosting Environment | Development | Quality | Production |  |
| Solution Type | B2E | B2B |  |
| Line of Business | Group | Hudson |  |
| Service identifier | CORPAPPS | ERP | INFRA | STORESYSTEMS |  |
| Application Id | DUFWVD | HUDMD |  |
| Country Cost Center | 1889 |  |
| Budget Plan | BP0053081 | BP0054159 | \* |  |
| Project Number | PRJ00040156 | PRJ00065611 | \* |  |
| Maintenance Windows | Weekends | \* |  |

* 1. Identity and access management

An Azure AD tenant provides identity and access management, which is a kay part of organization security posture. An Azure AD tenant ensures that authenticated and authorized users only access the resources to which they have permissions.

* + 1. Corporate identity synchronization

Dufry incorporates one Azure AD Tenant with identity synchronization from on-premises Active Directory Domain Services via Azure AD Connect. Users have a single account across on-premises and Azure AD federated resources (such as Microsoft 365).

Text

Description automatically generated with medium confidence

* + 1. Authentication and authorization services/features

The following services/features are used to help users authenticate and authorize access to Azure resources:

* Username & Password + Azure AD MFA
* Azure AD Privileged Identity Management

IT administrators and VIP users are applied those services/features.

* + 1. Emergency access accounts

There is Implemented and configured break glass account for Azure AD:

* Break.Glass@dufry.com

It is excluded from MFA and Conditional Access polices and has an Azure AD PIM permanent role assignment of Global Admin to Azure AD.

* + 1. Monitoring, logging, and alerting

All Azure AD audit & sign-in logs are sent to a central Log Analytics workspace. Alerting is not configured.

* + 1. External users

External users, like partners, gain access to manage Azure resources within Azure subscriptions over Azure AD guest users (B2B) invitation into our Azure AD tenant.

* + 1. Access to resources

Access to resources in Azure environments is granted via Azure RBAC (IAM). RBAC assignments are only given to groups (cloud only or synchronized). Users are added to the groups.

Only built-in RBAC roles are assigned. These roles assign numerous built-in roles multiple times to tightly scope and control permissions and ensure that only required permissions are given.

* 1. Network topology and connectivity
     1. Virtual networks

Dufry organization deployed resources across multiple subscriptions and Azure regions. While some traffic across Azure regions is expected (such as traffic between two virtual networks across two different Azure regions), there is not required a full mesh network across all Azure regions.

Dufry organization followings the principle of "traffic in Azure stays in Azure" so that communication across resources in Azure occurs via the Microsoft backbone network, even when the resources are in different regions.

A picture containing timeline

Description automatically generated

Ref.: [Dufry\_Azure\_Landing\_Zone\_LLD\_v0.1-NET.png](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ref/Dufry_Azure_Landing_Zone_LLD_v0.1-NET.png?csf=1&web=1&e=gdfLTS)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Resource group | Location | Subscription |
| NetworkWatcherRG-vnet | networkwatcherrg | West Europe | DUFRY\_MASTERDATA |
| RG-MachineLearning-RubenPertusa-Lopez-vnet | rg-machinelearning-rubenpertusa-lopez | West Europe | DUFRY Production |
| VNET-DUF-MASTERDATA-PROD | rg-duf-masterdata-prod | West Europe | DUFRY\_MASTERDATA |
| vnet-duf-weu-corpapps-docandtraining-non-prod | rg-duf-weu-corpapps-docandtraining-dev | West Europe | duf-corpapps-non-prod |
| vnet-duf-weu-corpapps-infra-non-prod | rg-duf-weu-corpapps-infra-non-prod | West Europe | duf-corpapps-non-prod |
| vnet-duf-weu-corpapps-nonprod | rg-duf-weu-corpapps-infra | West Europe | duf-corpapps-001 |
| vnet-duf-weu-corpapps-prod | rg-duf-weu-corpapps-infra | West Europe | duf-corpapps-001 |
| vnet-duf-weu-erp-app-nonprod | rg-duf-weu-erp-infra | West Europe | duf-erp-001 |
| vnet-duf-weu-erp-app-prod | rg-duf-weu-erp-infra | West Europe | duf-erp-001 |
| vnet-duf-weu-infra | rg-duf-weu-infra-hub-prod | West Europe | duf-infra-001 |
| vnet-duf-weu-infra-app-dmz | rg-duf-weu-infra-app | West Europe | duf-infra-001 |
| vnet-duf-weu-infra-app-nonprod | rg-duf-weu-infra-app | West Europe | duf-infra-001 |
| vnet-duf-weu-infra-app-pci | rg-duf-weu-infra-app | West Europe | duf-infra-001 |
| vnet-duf-weu-infra-app-prod | rg-duf-weu-infra-app | West Europe | duf-infra-001 |
| vnet-duf-weu-infra-wvd-prod | rg-duf-weu-infra-hub-prod | West Europe | duf-infra-001 |
| vnet-duf-weu-security-non-prod | rg-duf-weu-security-infra-non-prod | West Europe | duf-security-non-prod |
| vnet-duf-weu-security-prod | rg-duf-weu-security-infra-prod | West Europe | duf-security-prod |
| vnet-duf-weu-storesystems-non-prod | rg-duf-weu-storesystems-infra-non-prod | West Europe | duf-storesystems-non-prod |
| vnet-duf-weu-storesystems-prod | rg-duf-weu-storesystems-infra-prod | West Europe | duf-storesystems-prod |
| vnet-hud-eus-corpapps-app-nonprod | rg-hud-eus-corpapps-infra | East US | hud-corpapps-001 |
| vnet-hud-eus-corpapps-app-prod | rg-hud-eus-corpapps-infra | East US | hud-corpapps-001 |
| VNET-WEU-PROD | rg\_dufry\_foundation\_prod | West Europe | DUFRY Production |
| VNET\_DUFRY\_DEV\_TEST\_POC | rg\_dufry\_foundation\_dev\_test\_poc | West Europe | DUFRY DEV/TEST/POC |

* + 1. Network topology

The topology is following a hub & spoke model with outside connectivity over the hub network only. Spokes only communicate via the hub, segregated by the central Azure firewall instance. This firewall instance is at the same time also part of the perimeter protection of the network.

Within the network zero trust principles are followed with the introduction of NSGs and optionally ASGs., with any-to-any rules not being allowed.

When a few of landing zones need to connect across regions and there is used global virtual network peering to directly connect landing zone spoke virtual networks to hub virtual network.

There is not used a hub and spoke topology based on Azure VWAN. Currently there is used private connectivity via VPN.

Graphical user interface, diagram

Description automatically generatedOn-premises datacenter connects to one virtual network hub in a West Europe Azure region.

Ref.: [Dufry\_Azure\_Landing\_Zone\_LLD\_v0.1-NET-HUB.png](https://dufry0.sharepoint.com/:i:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ref/Dufry_Azure_Landing_Zone_LLD_v0.1-NET-HUB.png?csf=1&web=1&e=9OTfxL)

|  |  |  |
| --- | --- | --- |
| Peer | Peer | Type |
| NetworkWatcherRG-vnet | <none> | <none> |
| RG-MachineLearning-RubenPertusa-Lopez-vnet | <none> | <none> |
| VNET-DUF-MASTERDATA-PROD | VNET-WEU-PROD | local |
| vnet-duf-weu-corpapps-docandtraining-non-prod | <none> | <none> |
| vnet-duf-weu-corpapps-infra-non-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-corpapps-nonprod | vnet-duf-weu-infra | local |
| vnet-duf-weu-corpapps-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-erp-app-nonprod | vnet-duf-weu-infra | local |
| vnet-duf-weu-erp-app-prod | vnet-duf-weu-infra | local |
| **vnet-duf-weu-infra (hub)** | vnet-duf-weu-corpapps-infra-non-prod  vnet-duf-weu-corpapps-nonprod  vnet-duf-weu-corpapps-prod  vnet-duf-weu-erp-app-nonprod  vnet-duf-weu-erp-app-prod  vnet-duf-weu-infra-app-dmz  vnet-duf-weu-infra-app-nonprod  vnet-duf-weu-infra-app-pci  vnet-duf-weu-infra-app-prod  vnet-duf-weu-infra-wvd-prod  vnet-duf-weu-security-non-prod  vnet-duf-weu-security-prod  vnet-duf-weu-storesystems-non-prod  vnet-duf-weu-storesystems-prod  vnet-hud-eus-corpapps-app-nonprod  vnet-hud-eus-corpapps-app-prod | local/global |
| vnet-duf-weu-infra-app-dmz | vnet-duf-weu-infra | local |
| vnet-duf-weu-infra-app-nonprod | vnet-duf-weu-infra | local |
| vnet-duf-weu-infra-app-pci | vnet-duf-weu-infra | local |
| vnet-duf-weu-infra-app-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-infra-wvd-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-security-non-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-security-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-storesystems-non-prod | vnet-duf-weu-infra | local |
| vnet-duf-weu-storesystems-prod | vnet-duf-weu-infra | local |
| vnet-hud-eus-corpapps-app-nonprod | vnet-duf-weu-infra | global |
| vnet-hud-eus-corpapps-app-prod | vnet-duf-weu-infra | global |
| **VNET-WEU-PROD (hub)** | VNET-DUF-MASTERDATA-PROD  VNET\_DUFRY\_DEV\_TEST\_POC | local |
| VNET\_DUFRY\_DEV\_TEST\_POC | VNET-WEU-PROD | local |

* + 1. IP addressing

Azure IP addressing schema provides flexibility, room for growth, and integration with on-premises networks. The schema ensures that communication works for deployed resources, minimizes public exposure of systems, and gives the organization flexibility in its network.

Strategy for assigning IP addresses to Azure:

* there are used use only private IP address ranges from RFC 1918 for private on-premises networks and Azure virtual networks
* there are not used any of the following IP address ranges as address space of Azure or on-premises networks: 224.0.0.0/4 (multicast), 255.255.255.255/32 (broadcast), 127.0.0.0/8 (loopback), 169.254.0.0/16 (link-local), and 168.63.129.16/32 (internal DNS)
* there are not created large Azure virtual networks like (/16), unless for landing zone virtual networks hosting services that may require thousands of IP addresses, such as Azure Kubernetes or Azure Databricks

[10.249.0.0\_Microsoft\_Azure\_North\_Europe.xlsx](https://dufry0.sharepoint.com/:x:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_ip/10.249.0.0_Microsoft_Azure_North_Europe.xlsx?d=wac7f7b7893214cb1972238f0550f7c53&csf=1&web=1&e=SCfOES)

* + 1. Connectivity to Azure PaaS services

Virtual network injection is used for supported Azure services to make them available from within virtual network, and the communication within the virtual network is locked down by using UDRs and NSGs:

* when available always private link endpoints for Azure PaaS services is used that do not require public access
* when virtual network Injection or private link endpoints are not available, service endpoints are used, only on the subnets that really need access to a particular Azure PaaS service

[duf-ep.xlsx](https://dufry0.sharepoint.com/:x:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_inventory/duf-ep.xlsx?d=wf76c36b3dd8d456a80d94cf39aaa1fa6&csf=1&web=1&e=IdBBXC)

* + 1. Connectivity from/to the internet

There following solutions are implemented to secure workloads from inbound HTTP/S connectivity from/to the internet:

* single region: Application Gateway v2 with WAF protection and policies enabled for secure delivery of external-facing HTTP/S applications, and deployed within the landing-zone virtual network and with the applications that they're securing
* multi-region: when using Azure Front Door and Application Gateway v2 to protect HTTP/S applications, WAF policies are used in Front Door and lock Application Gateway down to only receive traffic from Front Door
* Azure's default internet outbound (SNAT) for any scenario is not used.
* exposure of VM management ports to the internet us prevented by using NSG.
* Azure Bastion is used to access jump-box virtual machines for management purposes.
  + 1. Traffic protection

NSGs are used to help protect traffic across subnets.

Application teams use application security groups at the subnet-level to help protect multitier VMs within landing zones.

East/west traffic across the platform (traffic between landing zones) is managed by central Azure Firewall to filter traffic flows, as well as advanced firewall capabilities (TLS inspection, network intrusion detection and prevention system (IDPS), URL filtering, web categories), for all inbound connections and for East/west traffic filtering (when required).

NSG flow logs are enabled on all critical subnets in subscription as an audit-ability and security best practice.

[duf-flowlogs.xlsx](https://dufry0.sharepoint.com/:x:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_inventory/duf-flowlogs.xlsx?d=w28f5a83fe38247e3b71b4628ce44e54b&csf=1&web=1&e=H9AIIZ)

Use Network Watcher packets to capture despite the limited capture window.

* + 1. DNS name resolution

Azure Private DNS zones are created within a hub connectivity subscription. The zones include zones required for accessing Azure PaaS services via a private endpoint.

[duf-dns.xlsx](https://dufry0.sharepoint.com/:x:/r/sites/DufryHybridCloud/Shared%20Documents/General/07%20Operations/Azure%20Landing%20Zone%20LLD/_inventory/duf-dns.xlsx?d=w7b43e058a057439caa936456b2bda163&csf=1&web=1&e=AQGVe8)

Azure Private DNS zones are linked to virtual networks, and we use DNS servers as hybrid resolvers with conditional forwarding to on-premises DNS names (for example, dufry.com). We configure on-premises servers with conditional forwarders to resolver VMs in Azure for our Azure Private DNS zone (for example, azure.contoso.com).

* 1. Regulatory standards

Azure resource configuration evaluation for compliance is a manual process based on Microsoft Defender for Cloud recommendations:

Graphical user interface, application, Teams

Description automatically generated

To have mechanism in place to evaluate Azure resource configurations automatically and ensure compliance *BigID* product is considered, and initial phase of implementation started.

“Regulatory Compliance” tag is enforced by policies across all Azure resources.

* 1. Security standard

Security posture is calculated by Microsoft Defender for Cloud:

Graphical user interface, application, Word

Description automatically generated

Some Azure resources are integrated with our security assessment and on-prem SIEM solutions based on Splunk product.

Dufry organization has a well-defined process for assessing Azure service security configurations as well as monitoring, alerting, and integrating services with existing systems. Secure resource configurations are defined but not enforced.

* 1. Platform automation and DevOps

Management and deployment changes to Azure landing zone environments is done automatically, through a CI/CD pipeline, using Infrastructure-as-Code tools:

* Azure DevOps
* HashiCorp Terraform
* Azure Resource Manager

Graphical user interface, application, Teams

Description automatically generated

Code is stored centrally in a Git repository.

An infrastructure team deploys and manages platform resources like Management Groups, Policy, RBAC, Hub Networking & Hybrid Connectivity (like VPN), Identity, etc.

Infrastructure and application teams are encouraged to deploy resources in whatever way fits their requirements for achieving their goals and SLAs whilst using declarative Infrastructure-as-Code tooling. Teams work separately from each other in their own Git repository and CI/CD pipeline (or pipelines), which gives each team autonomy.

2. Abbreviations and definitions

|  |  |
| --- | --- |
| Abbreviation / term: | Meaning |
| API | Application Programming Interface |
| PIM | Azure API Management |
| ARM | Azure Resource Management |
| PaaS | Platform as a Service |
| POS | Point of Sale |
| VM | Virtual Machine |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| VPN | Virtual Private Network |
| WAF | Web Application Firewall |