Americana Last Mile Platform- Low Level Design

ALMP Cloud Infrastructure & Deployment

This document describes the Azure infrastructure and deployment architecture of ALMP.

Document Status:

Author: **Saravanan Venkatarathnam (Cognizant)**

Last updated: 05-06-2023

1. DOCUMENT INFORMATION

1.1 VERSION HISTORY

Version	*Date*	*Document Name*	*Role*	*Comments*
0.1	23/03/2023	Americana Last Mile Platform-Low Level Design	Architect	Initial document
0.2	11/05/2023	Americana Last Mile Platform-Low Level Design	Architect	DB information updated
0.3	05/06/2023	Americana Last Mile Platform-Low Level Design	Architect	DR details updated

Table 1 - Version history

1.2 REVIEW AND APPROVALS -AMERICANA

Ver sion	Date	Document Name	Role	Comments
0.3		Americana Last Mile Platform- Low Level Design	client	Initial document
0.2-		Americana Last Mile Platform- Low Level Design		

Table 2 - Review and approvals

1.3 DISTRIBUTION LIST

Version	Date	To
0.1	xx/dd/yyyy	Project team

Table 3 – Distribution List

1.4 STAKEHOLDERS

Name	Role/Title	Organization

Table 3 – Stakeholders List

1.5 DISCLAIMER

System and product names described in this document are not always accompanied by their Vendors or Owners trademark symbols (™, ®). It is hereby acknowledged that all trademarks are the property of their respective owners. Furthermore, any extracts from vendor documents implies that there is no intent not to acknowledge or violate any vendor’s copyrights.

Table of Contents

1. INTRODUCTION

This document outlines the detailed technical specification of ALMP Cloud platforms. The technical design depicts key infrastructure, cloud services and outlines its configurations as required for deploying and operating ALMP.

2. PURPOSE/AUDIENCE

This document is indented for architects, developers, and infrastructure stakeholders to understand implementation details of the Azure resources in ALMP platform. This document covers the build architecture and design detail to validate and support Integration functionalities for ALMP program.

3. GOALS AND OBJECTIVES

The overall cloud design for Americana targets for the following design goals:

- Greenfield implementation in Azure “UAE North” and “North Europe” regions to host ALMP platform.
- Development, Test, Production and DR environments will be provisioned in the target Azure cloud platform.
- Build a scalable IT Infrastructure
- Enabling Rapid deployment of IT services
- Implement a high level of self-deployment and automation of IT services
- Provide the right levels of Availability, Confidentiality, and Integrity (based on workload and requirements)
- Scalable and flexible Solution
- Next Gen Cloud Based Platform
- Agile and Fool Proof Organization
- Optimize Delivery Fleet
- Best in class Technology Solution
- Enhance support to vital areas of production.
- Leverage best practice from product.
- Leverage the potential for automation.
- Aim for separate Americana logistics company.

3.1 SCOPE

The following sections enlists the scope and out-of-scope of ALMP infrastructure and deployment requirements.

In Scope

1. Greenfield implementation in Azure UAE Central and North Europe regions to host ALMP platform.
2. Development, Test, Production and DR environments will be provisioned in the target Azure cloud platform.
3. Azure Resource Manager templates/Terraform script for deployment of Azure resources.
4. Azure AD established in the already existing Azure cloud hosting of Americana will be leveraged for this ALMP application/infrastructure authentication.
5. Azure Virtual Network features like Security Groups, Network Access Control List (ACLs) and Flow Logs will be leveraged to provide cloud native security to Azure resources. Security groups will act as a firewall for associated Azure Virtual Machines, controlling both inbound and outbound traffic at the instance level.
6. Containerized Java Spring boot Application of the target platform will be deployed through Azure AKS
7. Provisioning of Azure cloud resources and Automated Deployment (for Development, Test, Production and DR env) using ARM templates / Terraform script
8. Azure Native Monitoring and Backup Services
9. Azure native security services (NSG, ACL, etc.) enabling and configuring as per Americana requirement.
10. Azure Container Registry to store private Docker images, which are deployed to the cluster.
11. Prod environment uptime will be based on the Microsoft Service Agreement with Americana for the Azure platform.
12. While Cognizant will make best effort to meeting Americana desired uptime (99.999%), the actual uptime will be baselined during the design phase based on the design decision mutually agreed Americana and Cognizant
13. Azure “Traffic manager” managed service will redirect the traffic to the Azure UAE North region when system outage at UAE Central primary region occurs and through IaC the systems at DR site will be deployed /restarted to resume the platform services from DR site as per the RTO
14. Azure Storage security features that enable data to be secured at rest and in transit will be leveraged.
15. Azure PostgreSQL Database relational database-as-a-service in Azure, managed DB (PaaS) service will be leveraged for DB in Development, Test, Production and DR environments. Redis Cache for caching common data

16. Azure managed Batch services will be leveraged for batch process of the target cloud platform.
17. Azure Key Vault will be used to safeguard cryptographic keys and secrets that cloud applications and services use.
18. The native Azure Backup service will be used for backup & restoring and configured to meet Americana's desired retention policies and remote backup to DR site. Azure cold storage will be leveraged for long term data storage (archival) requirement of the cloud platform at the most cost-effective manner
19. Centralized log management into Azure log analytics
20. Leveraging Azure automation logs from log analytics will be retained as per Americana compliance requirement
21. Azure Monitor service will be leveraged for monitoring the infrastructure provisioned and the application deployed in Azure cloud.

Out of Scope

1. Existing Home Delivery solutions enhancements and support
2. Building MDM solution, Metadata Management, Data Profiling/Quality Rules Engine, Data Governance platform
3. Language support other than English and Arabic.
4. OCM is out of scope except only training material creation
5. Cloud Hosting and Management services
6. Production support (Run) for the new Product barring Hypercare support
7. GIS / Map Data (POI/Street Network/Area Boundaries) procurement or creation and maintenance
8. Any kind of real time driver position testing in the navigation map.
9. Any kind server configuration for MPOS transaction for the delivery order
10. Procurement of Google Maps or other Mapping Services providers licenses for consumption by the applications
11. User Acceptance Testing. UAT would be executed by Business users. Cognizant would support in issue resolution.
12. Any changes in external systems that need integrations with ALMP
13. Addressing any Performance/Security/NFR Compliance introduced due to non-Cognizant developed components.
14. Reverse Engineering of the existing system not planned for data extraction or other activities
15. Infra Penetration Testing and Infrastructure Operational Acceptance Testin
16. AI/ML Downstream systems integration
17. Data Privacy Implementation for Americana as an organization
18. Active Directory set up and configuration.
19. Assessment and setting up of infra/cloud services other than Azure.
20. Data residency assessment.
21. Assessment and setting up Confluent and other third-party services.
22. Helpdesk support
23. Tools or solutions not implemented by Cognizant.

24. Security and Compliance (such as HIPPA, SOX, ISO, PCI)
25. Any configurations / changes at Americana On-Premises datacentres
26. Environment and Test data management is out of scope for all internal /external applications that shall be integrated with ALMP.
27. Procurement of all third-party tools, cloud infrastructure, cloud resources including licensing and subscription shall be the responsibility of Client.
28. Implementation and use of any Cognizant propriety tools/IP are not considered for this program
29. SLA's will not be applicable during 12 weeks of hyper care support post every Go-Live
30. Post Hypercare/Steady state support is out of scope.
31. Anything not expressly mentioned as an in-scope item under the scope sections above

3.2 REQUIREMENTS, ASSUMPTIONS AND PRE-CONDITIONS

Functional requirements

- **Security and Privacy**

✓ Personal Data Protection
✓ Security issues reporting
✓ Automated source code analysis
✓ Data privacy by design
✓ SAST, DAST and IAST

- **Disaster Recovery**

✓ Recovery Time Objective
✓ Recovery Point Objective
✓ Load Balancer with high availability and Cross Regional Data Centers

- **Azure Infrastructure**

✓ Azure Foundation Setup & Configuration for - Development, Test, Production and DR env.
✓ AKS clusters, Azure Container registry setup using ARM templates/Terraform script
✓ Provisioning of Azure cloud resources, AKS clusters and Infrastructure Automation for Development, Test, Production and DR env. using ARM templates / Terraform script
✓ Design document for the environments mentioned for AKS implementation.
✓ Provisioning and enabling of other relevant required Azure services like – Azure Monitor, Azure Container Registry, Azure Batch, Azure Log analytics,
✓ Provisioning of Azure managed PaaS DB services like Postgres DB & Mongo Atlas DB
✓ Setup Azure Native Monitoring and Backup Services
✓ Azure native security services (NSG, ACL, etc.) enabling and configuring as per Americana requirement.
✓ Sign-off on OCM deliverables from the Americana within one week of submission.

Pre-conditions

- ✓ The project team will get full enterprise admin access to the Americana enterprise portal ea.azure.com;
- ✓ Americana to deliver a cost center structure, organizational structure for the cloud enterprise structure design.

Assumptions

- **GENERAL**

- ✓ Any scope change will be assessed for impact and extension of project will be discussed mutually with Americana
- ✓ Extension to timelines or effort due to scope change or delay in the stakeholders consensus on requirements, or documentation unavailability (Current state etc.) will be managed via Change Request Process
- ✓ If certain design considerations result into the different tech stack choices/recommendations during the Foundation phase, additional cost impact has to be analyzed and agreed upon (if any)
- ✓ All Tools licenses, Cloud Subscriptions, will be provided by customer

- **INFRASTRUCTURE**
- ✓ Azure subscription will be owned and provided by Americana. Cognizant to leverage Americana Azure Subscription for the ALMP application target environment build in Azure Public cloud.
- ✓ All Software licenses required for installation of application/middleware/DB and for its replication at the Azure target environment shall be provided by Americana.
- ✓ Azure AD established in the already existing Azure cloud hosting of Americana will be leveraged for this ALMP application/infrastructure authentication purposes.
- ✓ Network Connectivity – Americana to own the network connectivity between On-premise and Azure target cloud. Cognizant to leverage the existing Americana on-prem to Azure Connectivity (Express route)
- ✓ Azure native security service(VNET,NSG, ACL) is to be leveraged for the Americana Azure target Infrastructure environment
- ✓ Americana will provide necessary access to its resources at on premise for any integration required from the cloud platform
- ✓ Americana to ensure availability and support of dependent teams from Americana during the implementation phase.
- ✓ Any deviation on effort and schedule commitments due to external team availability such as external vendors, provisioning of resources, Americana subject matter expert (SME) availability, environment downtime, delays in procuring approvals will be addressed through change management process
- ✓ Once the cloud Infra setup of the individual env. (Dev,Test,Prod &DR) is signed off by the application team after their all sort of testing of that environment, the same will be taken over by client through their own IT team for the BAU support.

Dependencies

- **GENERAL**

- ✓ Availability of Americana Functional SMEs /Architects through out the course of the engagement for discussions, query resolutions and review process.
- ✓ Availability of Americana Product Manager throughout the course of the engagement for requirements definition, product backlog refinement and sprint prioritization
- ✓ Availability of VPN, user IDs, other details to start the work
- ✓ Infrastructure & Hardware to be provided by Americana for SMS and MPOS Testing
- ✓ All software licenses, devices, access to environments, and code repository and environment provisioning will be provided by the Americana
- ✓ All the necessary assets, tools, approvals and brand guidelines will be made available before commencement of development
- ✓ Americana SME time should be allotted for domain understanding, data understanding, model results and insights discussions and UAT
- ✓ Any communications to end users / stakeholders outside Americana / Americana's customers / supply partners is to be managed by Americana

4. SOLUTION OVERVIEW

ALMP Azure infrastructure build on the HUB and Spoke standard architecture. Hub and spoke is a networking model for efficiently managing common communication or security requirements. It also helps avoid Azure subscription limitations. The below diagram provides a high-level overview of Azure ALMP Deployment Architecture. The key components and its purposes are listed- in the following sections.

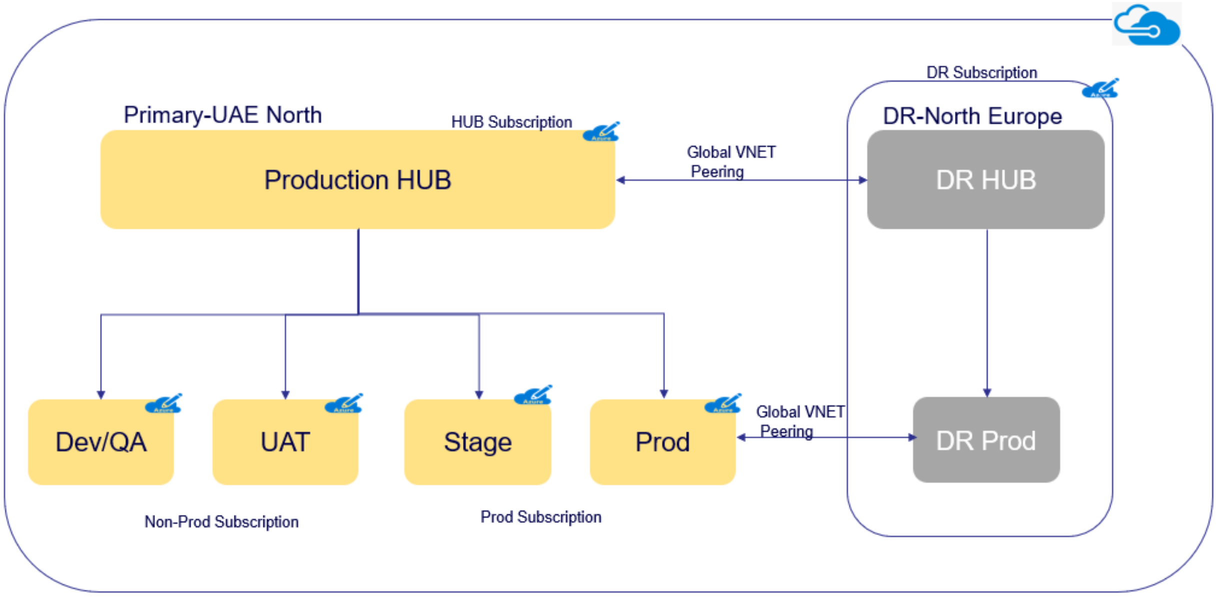


Figure 1: Azure Landscape Diagram

The subscriptions are segregated as below.

- HUB Subscription – Considered as a DMZ network contains public-facing services and is designed to help protect the internal networks for Primary and DR regions.
- Non-Prod Subscription – Contains non-production (Dev/QA/UAT) environment resources.
- Production Subscription – Comprised of Production environment resources.

Third Party Cloud Solutions

Below are the Third-party components integrated with ALMP, maintenance and troubleshooting managed by directly reaching the vendor.

Confluent
Payment service
Route mobile
Google API
Google Firebase
Acu weather

4.1 DESIGN DECISIONS

This section covers the key principles, which is considered for designing the Cloud foundation blocks for ALMP-

Design Area	Design Principle	Design decision
Azure Region	Resource availability.	Primary: UAE North Disaster Recovery: North Europe (Azure resources is not available in the "UAE North" paired region which is "UAE Ventral". Hence chosen "North Europe" as a DR region")
Azure Subscription	Centralized Billing and Chargeback	Multi-Subscription Model
	Overcome Azure Limits and Constraints	Hub and Spoke Subscription
	Azure Account	Owned by Americana
Logical Grouping	Management Groups and Azure Policy	Management groups needs to be created as defined in subsequent slides and apply policies (Based on the list provided which covers all of them).
	Group the applications in a logical container. Tag the resources for better management	Resource Groups - segregated based on environment. Resource Tags - Resource Labelling
	Resource Locks	Create locks for production resources, which restricts accidental deletion.

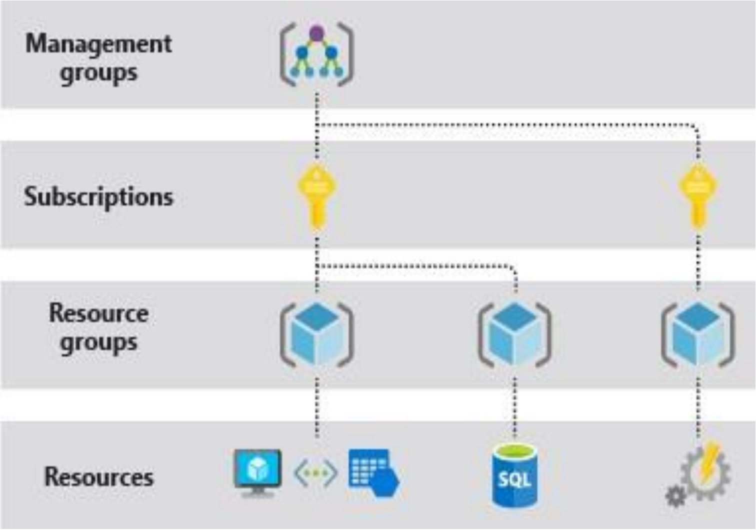
Security	Encryption- Encrypt Data at Rest using best possible way.	SSE- Storage Level (Azure Storage encryption is enabled for all storage accounts and cannot be disabled. Storage accounts are encrypted regardless of their performance tier (standard or premium)) Azure default encryption – Posgres DB Default encryption enabled
	Isolate the environments in security boundary. Restrict communication between production and non-production environments	All inbound traffic controlled by a dedicated "Application Gateway". Outbound traffic managed by Firewall and UDR mapped to each subnet.
	Hub and Spoke Model	Host common services in a centralized Subscription. Separate subscriptions for environments (Production and Nonproduction)

Network/ Security	Threat Management- Visibility into the possible threats and having more security control on the Azure resources	Azure Security Centre- Standard tier WAF – For all inbound requests. Firewall – For outbound requests
	Log Management, Event Co-relation, and analysis	Azure Monitor/ Log Analytics
	Endpoint Security	**Need to follow Americana end point security, currently no End point security configured**
High Availability	Service High Availability within the Azure region and gain maximum availability. Use Operating System Clustering and native application HA where possible	Deploy multiple instances of a service in Azure Availability Zones for Production resources in Primary region
Identity and Access Management	Controlled Access to the Azure resources.	Utilize existing Azure Active Directory/Domain Controllers for managing all the server instances.
		Authorization - Azure RBAC (Role Based Access Control)
Disaster Recovery	Availability of critical applications even when the primary region is offline due to any issues.	Host the ALMP application in 2 regions (UAE North and North Europe)
Monitoring	Monitor Platform and application availability etc. Integrate the monitoring solution with Event management tool and then to Service Management for Auto ticketing.	**New Relic**: used as a primary monitoring tool for all the resources. **Azure Monitor**: Cloud admins and core team can connect to portal to monitor the Azure resources. **Third party components:** Need to access the portal of the individual of the “third party” resources for all the monitoring requirement.

Subscription Management

The fundamental component of connecting to Azure is by deploying Azure Subscription and it is the administrative security boundary for the Azure Cloud Services. The subscription provides access to Azure resources and access to multiple services, and it provides the portal for managing the resources in Azure.

Cognizant proposes effective use of Azure Management Groups, Subscriptions, and Resource Groups to organize structure in Azure. Policies can be applied at any of these levels and the management groups can be nested as well.



ALMP follows multi-subscription model, which is based on the environments. Azure provides the flexibility to create multiple subscription. Multiple subscriptions help to overcome the limitation of single subscription and manage the resources more effectively. Multiple subscription also helps in providing more control on billing and chargeback as well.

As part of the ALMP build, it has been decided to build the cloud foundation in HUB and SPOKE model. All the common shared services will be hosted in the HUB and the application environments will be hosted in the SPOKE subscriptions. The spokes will be connected to the HUB using VNET peering.

Primary Region is UAE North

As there is an issue from Azure side to allocate the resources from "UAE central" region, hence "North Europe" enabled as a DR region based on the discussion with Americana and Microsoft.

Each environment resources are segregated based on subscription, Resource groups and Virtual network is intended to utilize Azure Resource Groups and VNet/Subnets to segregate application workloads into multiple environments such as Dev, QA, stage, Prod and DR.

Below table depicts the subscription names with hierarchy, which are in scope.

Subscription Name	Environment
ALMP-DEV-CSP	Development/QA
ALMP-UAT-CSP	UAT Testing
ALMP-HUB-CSP	Primary/DR HUB Resources
ALMP-PROD-CSP	Primary/DR Production

Resource groups

Azure Resource Group enables to work with the resources in the solution as a group. The benefits of resource groups are as follows.

- Manage all resources in an application/environment together as a group.
- Apply role-based access control (RBAC) to grant appropriate access to users, groups, and services.

ALMP designed multiple Resource groups based on the environment segregation, each resource groups hold all the resources that is required for an application.

The below mentioned resources groups have been created for the development environment of ALMP.

Resource Group Names	Region
rg-almp-prod-001	UAE North
rg-almp-uat-001	UAE North
rg-almp-np-001	UAE North

Azure Resource Tags

Resource Tags will be used for all the resources created in ALMP environment, this will help in identifying the resources and its usage. This approach helps in organizing resources for billing and charge back. Resource policies will be implemented to make sure that the resource tags consistency is available across the subscription. Additional tags can be added on an ongoing basis based on the needs of ALMP for specific purposes.

Name	Value
Application	ALMP
Environment	Production/Non-Prod/UAT/DR

ALMP Azure resource Naming standard

Naming convention in place ensures that all the resources have a standard name, which helps managing those resources. A naming convention should in place before creating anything in Azure.

ALMP followed "Naming Standard" for the Azure components are listed below.

Asset type	Scope	Naming Format
Resource group	Subscription	rg-<App or Service name>-<Subscription type>-<###>
Azure Virtual Network	Resource group	vnet-<environment>-<Region>-<###>
Subnet	Virtual network	snet-<environment>-<subregion>-<###>
Network security group	Subnet or NIC	nsg-<policy name or appname>-<###>
Public IP	Resource group	pip-<vm name or app name>-<Environment>-<subregion>-<###>
Azure Virtual Machines	Resource group	<vm><appname><###>
VM storage account	Global	stvm<performance type><appname or prodname><region><###>
DNS label	Global	<A record of vm>.[<region>.cloudapp.azure.com]
Azure Load Balancer	Resource group	lb-<app name or role><Environment><###>
NIC	Resource group	nic-<##>-<vmname>-<subscription><###>
Azure Functions	Resource group	func-<App Name>-<servicename>-<Environment>-<###>.[{azurewebsites.net}]
Redis Cache	Resource group	redis-<App Name>-<Environment>
Azure Database for PostgreSQL	Resource group	psql-<App Name>-<Environment>
Azure Storage account - general use	Resource group	st<storage name><###>
Azure Storage account - diagnostic logs	Resource group	stdiag<first 2 letters of subscription name and number><region><###>
Azure Kubernets Services	Resource group	aks-<App Name>-<Environment>-<###>
Azure Key Vault	Resource group	kv-<appname>-<Environment>-<001
Container registry	Resource group	cr-<appname>-Environment>-001
Log Analytics Workspace	Resource group	log-<appname>-Environment>-001
Applicatation Gateway	Resource group	agw-<appname>-<Environment>-001
api managmenet service	Resource group	apim-<appname>-<Environment>-001
Privatelink	Resource group	pl-<appname>-<resource type>-<environment>-001

Note: confluence link for ALMP naming standard details.
[Naming Standard for ALMP - Americana Last Mile Delivery Program - Confluence (atlassian.net)]

ALMP Azure Cloud Network services

This section covers the cloud network components build in Americana. Azure Cloud Network services comprises of multiple components that includes Virtual Networks, Subnets, Network Security Groups, User Defined Routes, etc.

The IP Address Range (CIDR) to setup a ALMP “VNet” is provided by Americana team from their Global Address range.

Virtual Network [VNet] is a logical isolation of the Azure cloud, Virtual networks are isolated from one another within and between subscriptions. As part of the Cloud foundation build, Cognizant will deploy multiple virtual networks for hosting production, UAT & Stage, non-production (QA & Development) and DR workloads. VNet peering will be configured for the VNet-to-VNet communication within the region. Global peering will be created for the communication between the VNets hosted in multiple regions. The VNets will be configured with default Azure DNS servers.

Each VNets will have multiple subnets based on the application tiers and its types.

Azure VNet and Subnet Details of non-prod listed below.

VNet/Subnet Name	CIDR	NSG	Route Table
vnet-np-almp-001	10.202.12.0/23 and 10.202.4.0/22		
snet-np-almp-aks-001	10.202.12.0/24	snet-np-almp-aks-001-nsg	
subet-np-almp-shared-001	10.202.13.0/26	subet-np-almp-shared-001	
snet-np-almp-psql-001	10.202.13.64/28	snet-np-almp-psql-001-nsg	
snet-np-almp-apim-001	10.202.13.80/28	snet-np-almp-apim-001-nsg	snet-np-almp-apim-001-nsg
snet-np-almp-agw-001	10.202.13.96/28		
AzureBastionSubnet	10.202.13.128/26		
snet-np-almp-psql-flexi-001	10.202.13.192/27		
snet-np-almp-aks-syspod-001	10.202.4.0/22		

Azure VNet and Subnet details UAT listed below (Performance environment)

Vnet/Subnet Name	CIDR	NSG	Route Table
vnet-perf-uat-almp-001	10.203.32.0/20		
snet-perf-uat-almp-aks-syspod-001	10.203.32.0/21	snet-stage-almp-aks-syspod-nsg-001	rt-almp-perf-uat-fw-outbound-001
snet-perf-uat-almp-shared-001	10.203.40.0/26	subnet-uat-almp-shared-001	rt-almp-perf-uat-fw-outbound-001
snet-perf-uat-almp-psql-001	10.203.40.64/27	snet-uat-almp-psql-001-nsg	rt-almp-perf-uat-fw-outbound-001
snet-perf-uat-almp-aks-sysnode-001	10.203.40.96/27	snet-stage-almp-aksnode-001-nsg	rt-almp-perf-uat-fw-outbound-001
snet-uat-almp-psql-flexi-001	10.203.40.128/27		

Azure VNet and Subnet Details Stage environment listed below.

Vnet/Subnet Name	CIDR	NSG	RouteTable
vnet-stage-almp-001	10.203.16.0/20		
AzureBastionSubnet	10.203.24.128/26		
snet-stage-almp-aks-syspod-001	10.203.16.0/21	snet-stage-almp-aks-syspod-nsg-001	rt-uat-stage-almp-outbound-001
snet-stage-almp-shared-001	10.203.24.0/26	subnet-stage-almp-shared-001	rt-uat-stage-almp-outbound-001
snet-stage-almp-psql-001	10.203.24.64/27	snet-stage-almp-psql-nsg-001	rt-uat-stage-almp-outbound-001
snet-stage-almp-aks-sysnode-001	10.203.24.96/27	snet-stage-almp-aksnode-001-nsg	rt-uat-stage-almp-outbound-001
snet-stage-almp-psql-flexi-001	10.203.24.192/27		

Azure VNet and Subnet Details Production environment listed below.

Vnet/Subnet Name	CIDR	NSG	RouteTable
vnet-prod-almp-001	10.203.0.0/20		
snet-prod-almp-aks-syspod-001	10.203.0.0/21	snet-prod-almp-aks-syspod-nsg-001	rt-almp-prod-fw-outbound-001
snet-prod-almp-shared-001	10.203.8.0/26	subnet-prod-almp-shared-001	rt-almp-prod-fw-outbound-001
snet-prod-almp-psql-001	10.203.8.64/27	snet-prod-almp-psql-nsg-001	rt-almp-prod-fw-outbound-001
snet-prod-almp-aks-sysnode-001	10.203.8.96/27	snet-prod-almp-aksnode-001-nsg	rt-almp-prod-fw-outbound-001
AzureBastionSubnet	10.203.8.128/26		
snet-prod-almp-psql-flexi-001	10.203.8.192/27		

Azure VNet and Subnet Details Primary HUB environment listed below

Vnet/Subnet Name	CIDR	NSG	RouteTable
vnet-hub-almp-001	10.202.8.0/22		
	10.202.14.0/23		
AzureFirewallSubnet	10.202.8.0/26		
snet-HUB-almp-prod-agw-001	10.202.8.64/26	snet-hub-almp-prod-apim-nsg-001	prod-almp-apim-route
snet-HUB-almp-prod-apim-001	10.202.8.128/26		
snet-HUB-almp-np-agw-001	10.202.8.192/27		
snet-HUB-almp-np-apim-001	10.202.8.224/27	snet-hub-almp-prod-apim-nsg-001	np-almp-apim-route
snet-HUB-almp-shared-pp1	10.202.9.0/27	snet-hub-almp-shared-nsg-001	hub-snet-almp-shared-pp1-route
snet-HUB-almp-kml-shared-001	10.202.9.32/27	snet-hub-almp-shared-nsg-001	hub-snet-almp-shared-pp1-route
snet-HUB-almp-stage-apim-001	10.202.9.64/26	snet-hub-almp-prod-apim-nsg-001	prod-almp-apim-route
snet-HUB-almp-stage-agw-001	10.202.9.128/26		
snet-HUB-almp-uat-perf-apim-001	10.202.9.192/26	snet-hub-almp-np-apim-nsg-001	
snet-HUB-almp-prod-standby-agw-001	10.202.10.0/25		
snet-HUB-almp-prod-apim-ha-001	10.202.10.128/26	snet-hub-almp-prod-apim-nsg-001	prod-almp-apim-ha-route
snet-HUB-almp-prod-apim-az-ha-001	10.202.11.0/26	snet-hub-almp-prod-apim-nsg-001	prod-almp-apim-ha-route
snet-HUB-almp-standby-apim-001	10.202.14.0/26	snet-hub-almp-prod-standby-apim-nsg-001	prod-almp-apim-route
snet-HUB-almp-standby-agw-001	10.202.14.64/26		
snet-HUB-almp-stage-apim-ha-test-001	10.202.14.128/26		
snet-HUB-almp-stage-agw-ha-test-001	10.202.14.192/27		

Azure VNet and Subnet Details DR HUB environment listed below.

Vnet/Subnet Name	CIDR	NSG	RouteTable
vnet-dr-hub-almp-001	10.202.0.0/22		
AzureFirewallSubnet	10.202.0.0/26		
snet-DR-HUB-almp-prod-agw-001	10.202.0.64/26		
snet-DR-HUB-almph-prod-apim-001	10.202.0.128/25		
snet-DR-HUB-almp-shared-pp1	10.202.1.0/27		

Azure VNet and Subnet Details DR Spoke environment listed below.

Vnet/Subnet Name	CIDR	NSG	RouteTable
vnet-dr-prod-almp-001	10.203.48.0/20		
snet-dr-prod-almp-aks-syspod-001	10.203.48.0/21		
snet-dr-prod-almp-shared-001	10.203.56.0/26		
snet-dr-prod-almp-psql-001	10.203.56.64/27		
snet-dr-prod-almp-aks-sysnode-001	10.203.56.96/27		

Note : Complete VNET and Subnet update in the below link.

VNet reserved for ALMP environment - Americana Last Mile Delivery Program - Confluence (atlassian.net)

Application Gateway

Azure Application Gateway is “Layer 7” web traffic load balancer, it can make a routing decisions based on additional attributes of an HTTP request. Application Gateway configured with Web Application Firewall (WAF) provides centralized protection of ALMP front end web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions.

AGW Name	HA Status	Public IP	Environment	Vnet/Subnet
agw-almp-hub-prod-ha-001	Enabled	20.233.113.30	PROD	vnet-hub-almp-001/snet-HUB-almp-prod-agw-ha-001
agw-almp-hub-np-001	Disabled	20.203.120.118	UAT	vnet-hub-almp-001/snet-HUB-almp-np-agw-001
agw-almp-hub-stage-001	Disabled	20.74.216.197	STAGE	vnet-hub-almp-001/snet-HUB-almp-stage-agw-001
agw-almp-np-001	Disabled	20.203.83.1	NON PROD	vnet-np-almp-001/snet-np-almp-agw-001
agw-almp-dr-prod-001	Enabled	20.105.97.197	DR PROD	vnet-dr-hub-almp-001/snet-dr-hub-almp-agw-001

The detailed WAF rules will be captured in the security document.

Note: The current WAF configured in ALMP is simply allow all the IPAAS traffic without any inspection.

API Management

The API gateway acts as a facade to the backend services, allowing API providers to abstract API implementations and evolve backend architecture without impacting API consumers. All requests from Application Gateway reach the API gateway and it acts as a single-entry point for all backend services and then forwards requests to respective backend services.

“Application Insights” configured for live metrics, end-to-end tracing, and troubleshooting.

APIM configured with “Virtual Network” and placed behind “Application Gateway” provides a network protection.

APIM Name	URL	Virtual Public IP	Tier	HA Status	Attached Subnet	Environment
apim-almp-hub-prod-ha-001	https://almp.americana.rest	20.203.68.160	Premium	Enabled	snet-HUB-almp-prod-apim-ha-001	PROD
apim-almp-dr-prod-001	https://apim-almp-dr-prod-001.azure-api.net	20.234.17.173	Premium	Enabled	snet-dr-hub-almp-apim-001	DR PROD
apim-almp-hub-stage-001	https://stage.americana.rest	20.233.31.10	Developer	Disabled	snet-HUB-almp-stage-apim-001	STAGE
apim-almp-hub-uat-perf-001	https://uat.americana.rest	20.203.43.237	Premium	Disabled	snet-HUB-almp-uat-perf-apim-001	UAT
apim-almp-np-01	https://qa.americana.rest	20.203.76.52	Developer	Disabled	snet-np-almp-apim-001	NON PROD

Azure Kubernetes services

Azure Kubernetes Service (AKS) is a managed service that allows to run Kubernetes orchestration service in Azure. AKS helps to simplify the deployment and management of microservices-based architecture and streamlines horizontal scaling, self-healing, load balancing, and secret management.

ALMP AKS build on Azure “Container Networking Interface (CNI)” network plugin , every pod gets an IP address from the subnet and can be accessed directly. Systems in the same virtual network as the AKS cluster see the pod IP as the source address for any traffic from the pod. Systems outside the AKS cluster virtual network sees the node IP as the source address for any traffic from the pod.

The maximum number of pods per node in an AKS cluster is 100.

Ingress controllers bring traffic into the AKS cluster by creating ingress rules and routes, providing application services with reverse proxying, traffic routing/load balancing, and TLS termination. This allows to evenly distribute traffic across the application services to ensure scalability and meet reliability requirements. ALMP application configured with “NGINX ingress controller” in the Azure Kubernetes Service (AKS) cluster.

AKS monitoring AKS monitoring performed via “Container insights”. Azure “Container Insights” has a native integration with AKS, like collecting critical metrics and logs, alerting on identified issues, and providing visualization, additional “new relic” monitoring tool configured with AKS metrics for Monitoring and alerting.

The details configuration for each cluster updated below

Production AKS Key configuration	
AKS Name	aks-almp-prod-001
Network Profile	CNI
AKS Subnet Node	snet-prod-almp-aks-sysnode-001
AKS subnet Pod	snet-prod-almp-aks-syspod-001
Max Pods per Node	100
Network Policy	Azure
Monitor	Azure Monitor /New relic
Ingress	Nginx (Opensource)
Node Count	7
Node Size	Standard_D32s_v3

UAT AKS Key configuration	
AKS Name	aks-almp-perf-uat-001
Network Profile	CNI
AKS Subnet Node	snet-perf-uat-almp-aks-sysnode-001
AKS subnet Pod	snet-perf-uat-almp-aks-syspod-001
Max Pods per Node	100
Network Policy	Azure
Monitor	Azure Monitor /New relic
Ingress	Nginx (Opensource)
Node Count	6
Node Size	Standard_D32s_v3

Stage AKS Key configuration	
AKS Name	aks-almp-stage-001
Network Profile	CNI
AKS Subnet Node	snet-stage-almp-aks-sysnode-001
AKS subnet Pod	snet-stage-almp-aks-syspod-001
Max Pods per Node	100
Network Policy	Azure
Monitor	Azure Monitor /New relic
Ingress	Nginx (Opensource)
Node Count	3
Node Size	Standard_D32s_v3

Non-Prod AKS Key configuration	
AKS Name	aks-almp-np-001
Network Profile	CNI
AKS Subnet Node	snet-np-almp-aks-001
AKS subnet Pod	NA
Max Pods per Node	30
Network Policy	Azure
Monitor	Azure Monitor /New relic
Ingress	Nginx (Opensource)
Node Count	7
Node Size	Standard_D4s_v3

DR Prod Resources	
AKS Name	aks-almp-dr-prod-001
Network Profile	CNI
AKS Subnet Node	snet-dr-prod-almp-aks-sysnode-001
AKS subnet Pod	snet-dr-prod-almp-aks-sysnode-001
Max Pods per Node	30
Network Policy	Azure
Monitor	Azure Monitor /New relic
Ingress	Nginx (Opensource)
Node Count	7
Node Size	Standard_D4s_v3

ALMP Azure Posgres SQL Flexi server

Azure Database for PostgreSQL is a relational database service in the Azure cloud built on the PostgreSQL open-source relational database

Azure Database for PostgreSQL - Flexible Server provides a zone resilient HA. The read replica feature allows to replicate data from an Azure Database for PostgreSQL server to a read-only replica, Cross-region replication created on Production workloads between “UAE-North” and “North-Europe” which is helpful for scenarios like disaster recovery.

ALMP Prod “Posgres DB” details listed below.

PSQL Name	HA Status	Configuration	Subnet	Storage	Private DNS
psql-flexi-almp-prod-001	Enabled	GP_Standard_D64ds_v4	snet-prod-almp-psql-flexi-001	512GB	psqlflexicoredns.postgres.database.azure.com
psql-flexi-analytics-almp-prod-001	Enabled	GP_Standard_D64ds_v4	snet-prod-almp-psql-flexi-002	512GB	psqlflexianalyticspdns.postgres.database.azure.com
psql-flexi-kafka-almp-prod-001	Enabled	GP_Standard_D64ds_v4	snet-prod-almp-psql-flexi-003	512GB	psqlflexikafkadns.postgres.database.azure.com
psql-flexi-rider-locupdates-almp-prod-001	Enabled	GP_Standard_D64ds_v4	snet-prod-almp-psql-flexi-004	512GB	psqlflexiriderdns.postgres.database.azure.com

ALMP “Non-Prod” “Posgres DB” details listed below.

PSQL Name	HA Status	Configuration	Subnet	Storage	Private DNS
psql-flexi-almp-np-01	Enabled	GP_Standard_D2ds_v4	snet-np-almp-psql-flexi-001	128GB	psqlflexiorderallocationdns.postgres.database.azure.com

ALMP “UAT (Performance)” “Posgres DB” details listed below.

PSQL Name	HA Status	Configuration	Subnet	Storage	Private DNS
psql-flexi-almp-uat-001	Disabled	GP_Standard_D64ds_v4	snet-uat-almp-psql-flexi-001	256GB	psqlflexicoredns.postgres.database.azure.com
psql-flexi-analytics-almp-uat-001	Disabled	GP_Standard_D64ds_v4	snet-uat-almp-psql-flexi-001	256GB	psqlflexikafkadns.postgres.database.azure.com
psql-flexi-kafka-almp-uat-001	Disabled	GP_Standard_D64ds_v4	snet-uat-almp-psql-flexi-001	256GB	psqlflexikafkadns.postgres.database.azure.com

Azure Key vault

Azure Key Vault Premium SKU is used to Securely store and tightly control access to passwords, certificates, API keys, and other secrets.

KeyVault Name	SKU	Environment	Access
kv-almp-hub-001	Premium	HUB	Allow public access from specific virtual networks and IP addresses
kv-almp-np-01	Premium	Non Prod	Allow public access from specific virtual networks and IP addresses
kv-almp-prod-001	Premium	PROD	Allow public access from specific virtual networks and IP addresses
kv-almp-prod-psql-backup	Premium	PROD	Allow public access from specific virtual networks and IP addresses
kv-almp-stage-001	Premium	STAGE	Allow public access from specific virtual networks and IP addresses
kv-almp-uat-01	Premium	UAT	Allow public access from specific virtual networks and IP addresses
kv-hub-almp-np-001	Premium	HUB(Non PROD)	Allow public access from specific virtual networks and IP addresses

ALMP Dashboard UI application Virtual machines

Virtual Machines used to administrate the ALMP PAAS resources like aks and DB instances.

Couple VM delicately created to host the UI Dashboard application. Below are the VM list.

VM Name	Size	Subnet	Firewall IP/ Port	Hardening	HA Status
VMALMPMGTDRPROD001	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-dr-prod-almp-001/snet-dr-prod-almp-shared-001	20.93.10.233/21058	CIS Image	Disabled
VMALMPMGTHUB001	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-hub-almp-001/snet-HUB-almp-shared-pp1	20.233.145.144/23012	No	Disabled
VMALMPMGTPROD002	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-prod-almp-001/snet-prod-almp-shared-001	20.233.145.144/26052	No	Disabled
VMALMPMGTNP001	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-np-almp-001/subet-np-almp-shared-001	20.216.24.98/22	No	Disabled
VMALMPMGTUATPERF001	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-perf-uat-almp-001/snet-perf-uat-almp-shared-001	20.233.145.144/12023	No	Disabled
VMALMPUIPROD01	Standard D4s v3 (4 vcpus, 16 GiB memory)	vnet-hub-almp-001/snet-HUB-almp-shared-pp1	20.233.145.144/17819	No	Enabled
VMALMPUIPROD02	Standard D4s v3 (4 vcpus, 16 GiB memory)	Standard D4s v3 (4 vcpus, 16 GiB memory)	20.233.145.144/18901	No	Enabled

ALMP Azure Cloud storage

Azure storage is a managed cloud services from Microsoft, like any other services Azure storage is high available, secure, durable, and redundant. Azure storage service consists of Blob storage, File storage, Queue storage, Table storage Disk storage etc. where we need to create and manage Azure storage accounts. Azure also provides managed disk storage where we don't need to create or manage storage accounts, this will be taken care by Microsoft themselves.

Managed premium disks will be used for all the servers in the environment, this will provide the consistency across the board and also provides extended SLA (99.9%) for single instance virtual machine. Azure Blob Storage will be used for storing backups and diagnostic logs. Azure Service Endpoints will be used to route storage traffic from internal network to storage services bypassing the internet route. Microsoft Azure storage provides adequate IOPS that meets application demand, it is recommended to choose the right compute series and storage tiers according to the requirement.

Storage Account Name	Type	HA Status	Public Access	Private endpoint
saalmpinfradevopsdrprodd	Standard/StorageV2 (general purpose v2)	Zone-redundant storage (ZRS)	Disabled	pl-sa-infra-devops-almp-dr-prod
saalmpinfradevopsnp	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Enabled for specific Vnet and IP	
saalmpinfradevopsprod	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Disabled	pl-almp-storage-acc-infradevops-prod-001
saalmpinfradevopsstage	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Disabled	
saalmpinfradevopsuat	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Enabled for specific Vnet and IP	pl-sa-infra-devops-almp-uat-001
stipaasalmpnp01	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Enabled for specific Vnet and IP	stipaasalmpnp01-Privateendpoint
stipaasalmpprod01	Standard/StorageV2 (general purpose v2)	Zone-redundant storage (ZRS)	Enabled for specific Vnet and IP	pl-almp-storage-acc-prod-001
stipaasalmpstage01	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Disabled	
stipaasalmpuat01	Standard/StorageV2 (general purpose v2)	Locally-redundant storage (LRS)	Enabled for specific Vnet and IP	stipaasalmpuatperf01-privateendpoint
stkmlalmphub01	Standard/StorageV2 (general purpose v2)	Zone-redundant storage (ZRS)	Disabled	pl-sa-stkml-almo-hub-001
stkmlalmphub02	Standard/StorageV2 (general purpose v2)	Zone-redundant storage (ZRS)	Disabled	pl-almp-hub-kml-sa-001

Azure resource locks

Resource Locks “Delete” will be used for all the resources that create in ALMP Azure environment to prevent from accidental deletion and modifications.

Identity and Access Management

Azure resources including azure portal access, authentication and authorization is governed through Azure Active Directory. Microsoft Azure Active Directory [AAD] is an identity and access management administered by Americana team.

Role Based Access Control (RBAC)

Cognizant utilizes Azure Active Directory (AAD) as the identity and access management solution for authentication and authorization to Azure portal and accessing Cloud resources.

The owner permissions will be retained by Americana team itself; Cloud Solutions Architects from Cognizant will be provided with Contributor access. In ALMP the access control of the Cloud resources will be managed and governed based on Resource Groups. The resources will be isolated in respective Resource Groups.

ALMP Azure Container Registry

Azure Container Registry is a private registry service for building, storing, and managing container images and related artifacts.

Container Registry Name	SKU	Private Endpoint	Environment
cralmpdrprod001	Premium	pl-cr-almp-dr-prod-001	DR PROD
cralmpnp001	Premium	pl-almp-cr-np-001	NON-PROD
cralmpprod001	Premium	pl-almp-cr-prod-001	PROD
cralmpstage001	Premium	pl-amlp-cr-stage-01	STAGE
cralmpuat001	Premium	pl-amlp-cr-uat-perf-01	UAT

5.1 AZURE SOLUTION ARCHITECTURE (LOGICAL)

This section provides a detailed overview on the logical/service components of Azure being planned at datacenter on a high level.

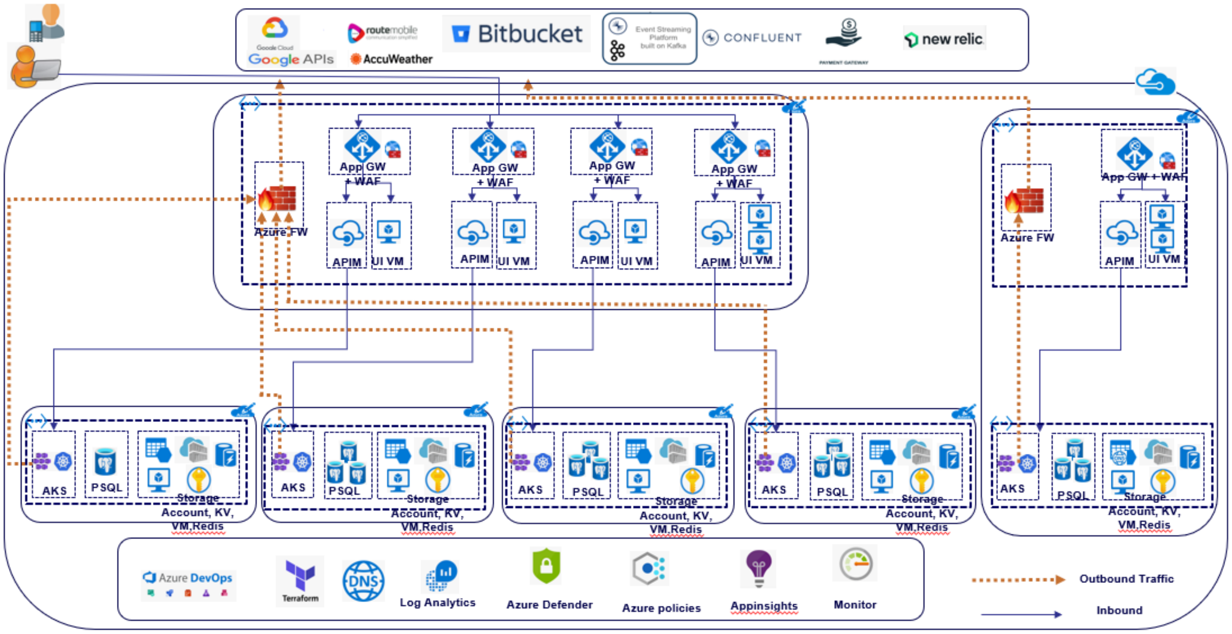


Figure 3: Azure service components all Environments.

Cognizant intend to follow an iterative architecture by initially building the Cloud foundation for hosting ALMP applications. The applications will be hosted in Azure **UAE-North** region being the primary region and **North-Europe** being the DR region.

Cognizant will consume ALMP provided Azure Subscription to avail Azure services, Cognizant propose to build the Cloud foundation with Hub and Spoke Model, the key benefit of this topology is as below.

- Cost savings by centralizing services that can be shared by multiple workloads in a single location.
- Separation of concerns
- Overcome Subscription limits.
- Scalable for future growth

Hub Subscription will be deployed with one virtual network per region (one in UAE-North and other in DR North Europe) for hosting shared services that will be consumed by all the application environments. Spoke subscriptions will hosts networks for application environment, below are the application environments.

- Dev/QA
- UAT
- Stage (AKA) Pre-prod
- Prod
- DR

Design Decisions

- Internet inbound traffic routed via application gateway and inspected by “Web application firewall”.
- Internet outbound traffic managed through firewall.
- “Route table” attached to each subnet (except api management and App GW) ensure all the outbound internet traffic inspected by firewall.
- API management configured with VNET integration ensures all the APIs are managed via private network.
- Network supported PAAS resources are attached with Private endpoint connection to ensure the private network flow.
- AKS will be hosted in a dedicated subnet with CNI network profile, the additional security feature will be applied based on Microsoft best practices.
- Postgres SQL hosted in a delegated subnet which provides an additional restriction for the resources to access the DB resources.
- Azure native monitoring tool used for monitoring the resources.
- NSG attached to each subnet and additional rules will be created based on the requirement.

Architecture design decision captured in the below link.

Infrastructure architecture design record - Americana Last Mile Delivery Program - Confluence (atlassian.net)

Assumptions

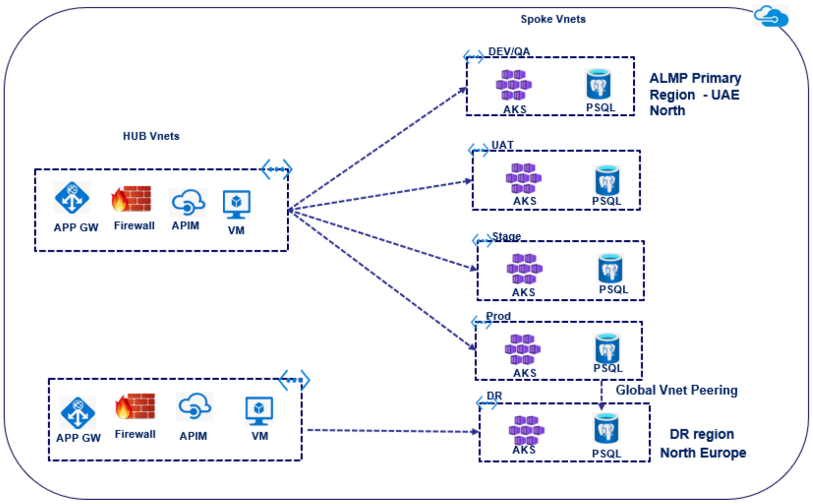
- Considering **UAE North** as a primary region and **North Europe** considered as DR region.
- Infrastructure components provisioning will be done using “**Azure devops”** pipelines, using Terraform IAC code.
- Existing Active directory setup leveraged for Azure identity and RBAC management.
- Azure “PosgreSQL” database will be replicated to a target DR region via “read replica” mode.
- No on-premises DNS used in this setup and FQDN resolution will be used via Azure DNS.
- Default Azure encryption used in all the resources.
- HA enabled only on the production resources.
- DR provisioned with Active/Passive approach.

5.2 AZURE DEPLOYMENT ARCHITECTURE

HUB and Spoke Architecture

A hub and spoke topology are a way to isolate workloads while sharing common services.

The hub virtual network is the central point of connectivity. It's a place to host services that can be consumed by the different workloads hosted in the spoke virtual networks.



As shown in the above diagram VNet hub environment comprises of shared resources, UI Dashboard VM and centralized security policy resources like firewall.

The spoke virtual networks are connected to the central hub environment through “Vnet to Vnet peering”. Shared services are deployed in the hub, while individual workloads are deployed inside spoke networks.

A separate HUB and Spoke environment are created in “North Europe” region for DR workloads. The DR spoke network is connected to the “Production” Virtual network via “VNet Peering” for enabling the DB replication between Production and DR regions.

PROD HUB Environment Components

Resource Name	Resources type	Region
afwalmphub001	Firewall	UAE North
agw-almp-hub-np-001	Application gateway	UAE North
agw-almp-hub-prod-ha-001	Application gateway	UAE North
agw-almp-hub-stage-001	Application gateway	UAE North
apim-almp-hub-np-001	API Management service	UAE North
apim-almp-hub-prod-ha-001	API Management service	UAE North
apim-almp-hub-stage-001	API Management service	UAE North
apim-almp-hub-uat-perf-001	API Management service	UAE North
appinsight-almp-hub-001	Application Insights	UAE North
AzureFirewallPolicy	Firewall Policy	UAE North
hub-snet-almp-shared-pp1-route	Route table	UAE North
INTERNETTESTROUTE	Route table	UAE North
kv-almp-hub-001	Key vault	UAE North
kv-hub-almp-np-001	Key vault	UAE North
loganalytics-ws-almp-hub-001	Log Analytics workspace	UAE North
MSVMI-loganalytics-ws-almp-hub-001	Data collection rule	UAE North
MyRouteTableRoute	Route table	UAE North
np-almp-apim-route	Route table	UAE North
pg-admon-poc	Virtual machine	UAE North
pip-vnet-hub-almp-001	Public IP address	UAE North
pl-almp-hub-kml-sa-001	Private endpoint	UAE North
pl-almp-keyvault-hub-001	Private endpoint	UAE North
pl-almp-keyvault-hub-np-001	Private endpoint	UAE North
pl-almp-storage-acc-kml-hub-001	Private endpoint	UAE North
pl-sa-stkml-almo-hub-001	Private endpoint	UAE North
privatelink.blob.core.windows.net	Private DNS zone	Global
privatelink.vaultcore.azure.net	Private DNS zone	Global
prod-almp-apim-ha-route	Route table	UAE North
prod-almp-apim-route	Route table	UAE North
prod-hub-almp-route	Route table	UAE North
snet-hub-almp-np-apim-nsg-001	Network security group	UAE North
snet-HUB-almp-prod-apim-001	Network security group	UAE North
snet-hub-almp-prod-apim-nsg-001	Network security group	UAE North
snet-hub-almp-prod-standby-apim-nsg-001	Network security group	UAE North
snet-hub-almp-shared-nsg-001	Network security group	UAE North
stalmpbootdiagnostic	Storage account	UAE North
stkmlalmphub01	Storage account	UAE North
stkmlalmphub02	Storage account	UAE North
TESTROUTE	Route table	UAE North
tm-almp-hub-prod-001	Traffic Manager profile	Global
tm-almp-stage-001	Traffic Manager profile	Global
VMALMPHUBMGMT001-nsg	Network security group	UAE North
VMALMPMGTHUB001	Virtual machine	UAE North
VMALMPMGTHUB001-ELB	Load balancer	UAE North
VMALMPUIPROD01	Virtual machine	UAE North

VMALMPUIPROD02	Virtual machine	UAE North
vnet-hub-almp-001	Virtual network	UAE North
waf-agw-hub-001	Application Gateway WAF policy	UAE North
waf-agw-hub-prod-001	Application Gateway WAF policy	UAE North
waf-agw-hub-prod-ha-001	Application Gateway WAF policy	UAE North
waf-agw-hub-prod-standby-001	Application Gateway WAF policy	UAE North
waf-agw-hub-stage-001	Application Gateway WAF policy	UAE North
waf-agw-hub-stage-002	Application Gateway WAF policy	UAE North

VNet reserved for ALMP environment - Americana Last Mile Delivery Program - Confluence (atlassian.net)

Dev/QA environment resources details

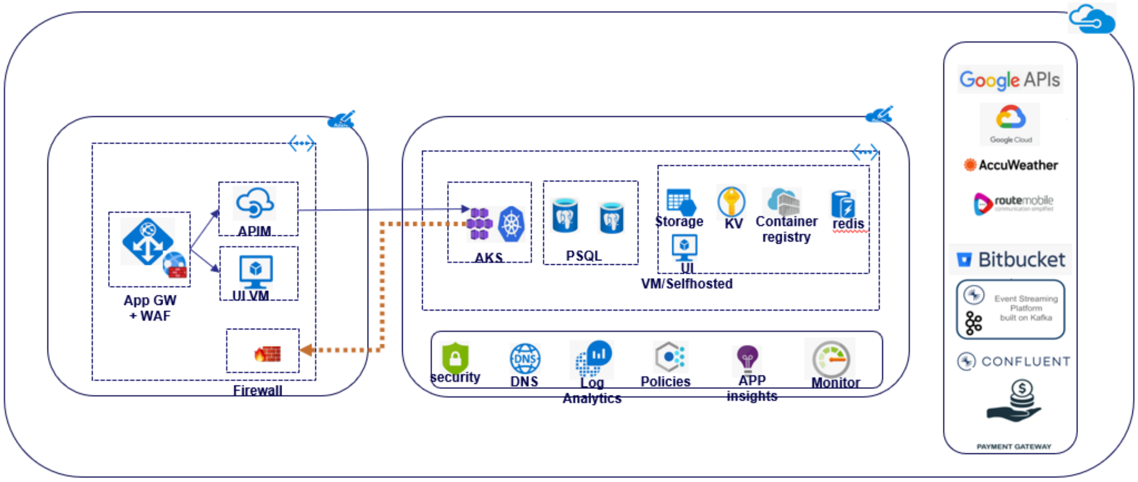


Figure 4: Azure service components Development

- Application gateway is configured with the WAF for inbound traffic.
- APIM Developer SKU selected for Dev/QA environment resources (Can be expanded dynamically).
- The ip address allocated to each subnet based on the SKU selected for Dev resources.
- Single “Posgres SQL Flexi” instances configured for Dev and QA workloads.
- AKS created with CNI profile.

Development/QA Environment Components

Resource Name	Resources type	Region
agw-almp-np-001	Application gateway	UAE North
agw-almp-np-pip	Public IP address	UAE North
aks-almp-np-001	Kubernetes service	UAE North
apim-almp-np-01	API Management service	UAE North
apim-almp-np-01-pip	Public IP address	UAE North
appinsight-almp-np-001	Application Insights	UAE North
azure-api.net	Private DNS zone	Global
cralmpnp001	Container registry	UAE North
dev-almp-apim-route	Route table	UAE North
dev-almp-fw-internetroute	Route table	UAE North
kv-almp-np-01	Key vault	UAE North
kv-almp-np-01	Private endpoint	UAE North
kv-almp-np-01-Privateendpoint	Private endpoint	UAE North
loganalytics-ws-almp-np-001	Log Analytics workspace	UAE North
pgadmin-poc	Virtual machine	UAE North
pgadmin-poc-pip	Public IP address	UAE North
pl-almp-cr-np-001	Private endpoint	UAE North
pl-almp-psql-analytics-np-001	Private endpoint	UAE North
pl-almp-psql-np-001	Private endpoint	UAE North
pl-almp-redis-np-001	Private endpoint	UAE North
pl-sa-almp-kml-np-001	Private endpoint	UAE North
privatelink.azurecr.io	Private DNS zone	Global
privatelink.blob.core.windows.net	Private DNS zone	Global
privatelink.postgres.database.azure.com	Private DNS zone	Global
privatelink.redis.cache.windows.net	Private DNS zone	Global
privatelink.vaultcore.azure.net	Private DNS zone	Global
psql-flexi-almp-np-01	Azure Database for PostgreSQL flexible server	UAE North
psqlflexianalyticsdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexidns.postgres.database.azure.com	Private DNS zone	Global
psqlflexigisdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexikorderdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexiorderaggregationdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexiorderallocationdns.postgres.database.azure.com	Private DNS zone	Global
qawebui-pip	Public IP address	UAE North
rediscache-almp-np-001	Azure Cache for Redis	UAE North
rt-test-vnet-peering-security	Route table	UAE North
saalmpinfradevopsnp	Storage account	UAE North
security-test-route	Route table	UAE North
selfhostedagent	Virtual machine	UAE North
selfhostedagent-ip	Load balancer	UAE North
selfhostedagent179	Network Interface	UAE North
snet-np-almp-agw-001-nsg	Network security group	UAE North

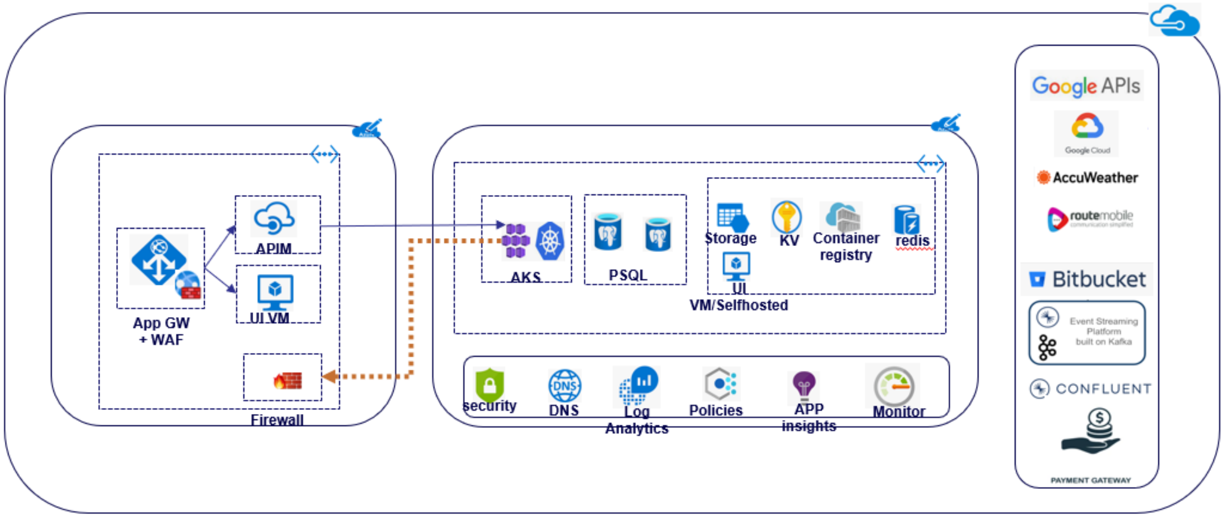
snet-np-almp-aks-001-nsg	Network security group	UAE North
snet-np-almp-apim-001-nsg	Network security group	UAE North
snet-np-almp-psql-001-nsg	Network security group	UAE North
sqldb-almp-np-001 (sqlserver-almp-np-001/sqldb-almp-np-001)	SQL database	UAE North
sqlserver-almp-np-001	SQL server	UAE North
stalmpkmlnp01	Storage account	UAE North
stdiagvmalmpnp01	Storage account	UAE North
stipaasalmpnp01	Storage account	UAE North
stipaasalmpnp01-Privateendpoint	Private endpoint	UAE North
stipaasalmpnp01-Privateendpoint.nic.1e94c6aa-06e8-48a8-8ddf-c17d416070b6	Network Interface	UAE North
subet-np-almp-shared-001	Network security group	UAE North
subnet-np-almp-agw-001	Network security group	UAE North
VMALMPMGTNP001	Virtual machine	UAE North
VMALMPMGTNP001-PIP	Public IP address	UAE North
VMALMPMGTNP01-ELB	Load balancer	UAE North
VMALMPUISERVERNP001-nsg	Network security group	UAE North
VMALMPUISERVERNP002-nsg	Network security group	UAE North
VMInsights(loganalytics-ws-almp-np-001)	Solution	UAE North
vmsecuritytestnsg	Network security group	UAE North
vnet-np-almp-001	Virtual network	UAE North
vnet-np-almp-001-bastion	Bastion	UAE North
vnet-np-almp-001-ip	Public IP address	UAE North

Azure Development environment resources - Americana Last Mile Delivery Program - Confluence (atlassian.net)

UAT environment resource details

UAT initially configured the SKU equivalent to Dev and later due to the performance requirement all the resources are upgraded and configured to match the production setup.

- Application gateway configured with the WAF for inbound traffic.
- APIM **Premium** SKU selected for UAT environment workloads.
- Three “PSQL Flexi server” configured to match the “Production” workload.
- AKS cluster built has been done with the exact match of production.



UAT Environment Components

Resource Name	Resources type	Region
aks-almp-perf-uat-001	Kubernetes service	UAE North
amlp-temp-vm	Virtual machine	UAE North
amlp-temp-vm990	Network Interface	UAE North
apim-almp-uat-01-pip	Public IP address	UAE North
azure-api.net	Private DNS zone	Global
cralmpuat001	Container registry	UAE North
kv-almp-uat-01	Key vault	UAE North
pe-almp-keyvault-uatperf-001	Private endpoint	UAE North
pe-almp-keyvault-uatperf-001-nic	Network Interface	UAE North
pl-almp-redis-cache-uatperf	Private endpoint	UAE North
pl-almp-redis-cache-uatperf-nic	Network Interface	UAE North
pl-almp-redis-uat-stage	Private endpoint	UAE North
pl-almp-redis-uat-stage-nic	Network Interface	UAE North
pl-amlp-cr-uat-perf-001	Private endpoint	UAE North
pl-amlp-cr-uat-perf-001-nic	Network Interface	UAE North
pl-amlp-cr-uat-perf-01	Private endpoint	UAE North
pl-amlp-cr-uat-perf-01-nic	Network Interface	UAE North
pl-psql-almp-uat-01-gis-idp-db	Private endpoint	UAE North
pl-psql-almp-uat-01-gis-idp-db-nic	Network Interface	UAE North
pl-psql-almp-uat-01-rider-tracking-locationupdates-db	Private endpoint	UAE North
pl-psql-almp-uat-01-rider-tracking-locationupdates-db-nic	Network Interface	UAE North
pl-psql-almp-uat-rider-locupdates	Private endpoint	UAE North
pl-psql-almp-uat-rider-locupdates-nic	Network Interface	UAE North
pl-psql-analytics-db-uat-001	Private endpoint	UAE North
pl-psql-analytics-db-uat-001-nic	Network Interface	UAE North
pl-psql-kafka-uat-001	Private endpoint	UAE North
pl-psql-kafka-uat-001-nic	Network Interface	UAE North

pl-sa-infra-devops-almp-uat-001	Private endpoint	UAE North
pl-sa-infra-devops-almp-uat-001-nic	Network Interface	UAE North
privatelink.azurecr.io	Private DNS zone	Global
privatelink.blob.core.windows.net	Private DNS zone	Global
privatelink.postgres.database.azure.com	Private DNS zone	Global
privatelink.redis.cache.windows.net	Private DNS zone	Global
privatelink.vaultcore.azure.net	Private DNS zone	Global
psql-almp-uat-perf-001-privateendpoint	Private endpoint	UAE North
psql-flexi-almp-uat-001	Azure Database for PostgreSQL flexible server	UAE North
psql-flexi-analytics-almp-uat-001	Azure Database for PostgreSQL flexible server	UAE North
psql-flexi-kafka-almp-uat-001	Azure Database for PostgreSQL flexible server	UAE North
psqlflexianalyticsdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexicoredns.postgres.database.azure.com	Private DNS zone	Global
psqlflexikafkadns.postgres.database.azure.com	Private DNS zone	Global
rediscache-almp-uat-001	Azure Cache for Redis	UAE North
rt-almp-perf-uat-fw-outbound-001	Route table	UAE North
saalmpinfradevopsuat	Storage account	UAE North
security-test-route-001	Route table	UAE North
snet-uat-almp-aks-001-nsg	Network security group	UAE North
snet-uat-almp-apim-001-nsg	Network security group	UAE North
snet-uat-almp-psql-001-nsg	Network security group	UAE North
snet-uat-almp-psql-flexi-001-nsg	Network security group	UAE North
snet-uat-almp-psql-flexi-nsg-001	Network security group	UAE North
stafdalmpuat001	Storage account	UAE North
stalmpvmdiagnostic	Storage account	UAE North
stipaasalmpuat01	Storage account	UAE North
stipaasalmpuatperf01-privateendpoint	Private endpoint	UAE North
stipaasalmpuatperf01-privateendpoint-nic	Network Interface	UAE North
subnet-uat-almp-shared-001	Network security group	UAE North
uat-almp-apim-route	Route table	UAE North
VMALMPMGTPERFUAT001-pip	Public IP address	UAE North
VMALMPMGTUAT001-ELB	Load balancer	UAE North
VMALMPMGTUAT001-pip	Public IP address	UAE North
VMALMPMGTUAT001_OsDisk_1_bde637afa71b488cb345ddbbfc25675d	Disk	UAE North
VMALMPMGTUATPERF001	Virtual machine	UAE North
VMALMPMGTUATPERF001-ELB	Load balancer	UAE North
vmalmpmgtuatperf001370	Network Interface	UAE North
VMALMPMGTUATTEMP001-nsg	Network security group	UAE North
VMALMPUISERVERUAT001-nsg	Network security group	UAE North
VMALMPUISERVERUAT002-nsg	Network security group	UAE North
vnet-perf-uat-almp-001	Virtual network	UAE North

Staging Environment Components

Stage environment acts as an interim “pre-prod” solution, it is created with the resources equivalent to prod.

Note: This environment current used for an adhoc testing, may be decommissioned later upon an agreement with Americana.

Resource Name	Resources type	Region
aks-almp-stage-001	Kubernetes service	UAE North
basicNsgvnet-stage-almp-001-nic01	Network security group	UAE North
cralmpstage001	Container registry	UAE North
kv-almp-stage-001	Key vault	UAE North
pl-almp-uat-stage-acr-001	Private endpoint	UAE North
pl-almp-uat-stage-acr-001.nic.12212a70-ee95-4592-aa68-e5d3d4bc285a	Network Interface	UAE North
pl-almp-uat-stage-kv-001	Private endpoint	UAE North
pl-almp-uat-stage-kv-001-nic	Network Interface	UAE North
pl-almp-uat-stage-psql-001	Private endpoint	UAE North
pl-almp-uat-stage-psql-001-nic	Network Interface	UAE North
pl-amlp-cr-stage-01	Private endpoint	UAE North
pl-amlp-cr-stage-01-nic	Network Interface	UAE North
pl-psql-almp-stage-analytics-001	Private endpoint	UAE North
pl-psql-almp-stage-analytics-001-nic	Network Interface	UAE North
privatelink.azurecr.io	Private DNS zone	Global
privatelink.postgres.database.azure.com	Private DNS zone	Global
privatelink.redis.cache.windows.net	Private DNS zone	Global
privatelink.vaultcore.azure.net	Private DNS zone	Global
psql-almp-stage-001	Azure Database for PostgreSQL single server	UAE North
psql-almp-stage-01-analytics-db	Azure Database for PostgreSQL single server	UAE North
psql-almp-stage-privateendpoint	Private endpoint	UAE North
psql-almp-stage-privateendpoint-nic	Network Interface	UAE North
rt-uat-stage-almp-outbound-001	Route table	UAE North
saalmpinfradevopsstage	Storage account	UAE North
selfhostedagentstaging	Virtual machine	UAE North
selfhostedagentstaging-ip	Public IP address	UAE North
selfhostedagentstaging-nsg	Network security group	UAE North
selfhostedagentstaging605	Network Interface	UAE North
selfhostedagentstaging_DataDisk_0	Disk	UAE North
selfhostedagentstaging_OsDisk_1_1b6be24069054c80b42e2a2f09c790f5	Disk	UAE North
snet-stage-almp-aks-syspod-nsg-001	Network security group	UAE North
snet-stage-almp-aksnode-001-nsg	Network security group	UAE North
snet-stage-almp-psql-nsg-001	Network security group	UAE North
stipaasalmpstage01	Storage account	UAE North
subnet-stage-almp-shared-001	Network security group	UAE North

ui-test-vm	Virtual machine scale set	UAE North
vnet-stage-almp-001	Virtual network	UAE North
vnet-stage-almp-001-bastion	Bastion	UAE North
vnet-stage-almp-001-ip	Public IP address	UAE North

Production

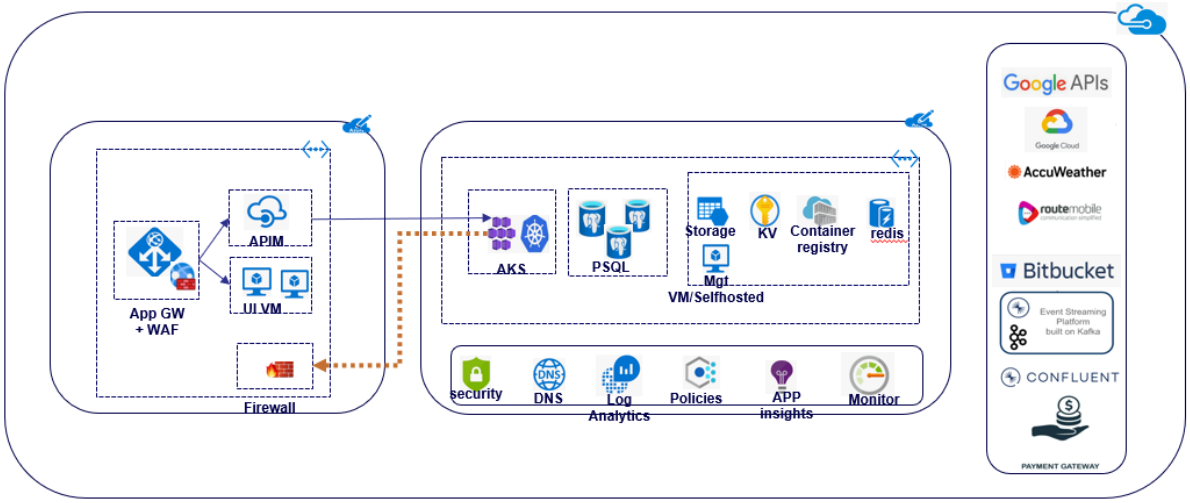


Figure 5: Azure service components Production.

Production resources planned carefully based on the analysis provided during the performance testing, all the resources in production are enabled with “high availability” and “scalability” on demand.

- Premium/ Standard SKU selected for Production environment resources.
- Internet Inbound traffic inspected by WAF.
- Outbound traffic to the external cloud is monitored and controlled by Firewall.
- Four PSQL instances created for production DB workloads with HA resilient.

PROD Environment Components

Resource Name	Resources type	Region
aks-almp-prod-001	Kubernetes service	UAE North
almp_prod_ssh_key	SSH key	UAE North
cralmpprod001	Container registry	UAE North
Ipass-storageccount-almp-prod-privateendpoint	Private endpoint	UAE North
Ipass-storageccount-almp-prod-privateendpoint-nic	Network Interface	UAE North
kv-almp-prod-001	Key vault	UAE North

kv-almp-prod-psql-backup	Key vault	UAE North
pe-almp-keyvault-prod-001	Private endpoint	UAE North
pl-almp-cr-prod-001	Private endpoint	UAE North
pl-almp-prod-psql-analytics-db-001	Private endpoint	UAE North
pl-almp-redis-prod-001	Private endpoint	UAE North
pl-almp-storage-acc-infradevops-prod-001	Private endpoint	UAE North
pl-almp-storage-acc-prod-001	Private endpoint	UAE North
pl-psql-almp-prod-rider-locupdates	Private endpoint	UAE North
privatelink.azurecr.io	Private DNS zone	Global
privatelink.blob.core.windows.net	Private DNS zone	Global
privatelink.database.windows.net	Private DNS zone	Global
privatelink.postgres.database.azure.com	Private DNS zone	Global
privatelink.redis.cache.windows.net	Private DNS zone	Global
privatelink.vaultcore.azure.net	Private DNS zone	Global
psql-almp-kafka-privateendpoint	Private endpoint	UAE North
psql-almp-prod-001	Azure Database for PostgreSQL single server	UAE North
psql-almp-prod-01-analytics-db	Azure Database for PostgreSQL single server	UAE North
psql-almp-prod-privateendpoint	Private endpoint	UAE North
psql-almp-prod-rider-locupdates	Azure Database for PostgreSQL single server	UAE North
psql-flexi-almp-prod-001	Azure Database for PostgreSQL flexible server	UAE North
psql-flexi-analytics-almp-prod-001	Azure Database for PostgreSQL flexible server	UAE North
psql-flexi-kafka-almp-prod-001	Azure Database for PostgreSQL flexible server	UAE North
psql-flexi-rider-locupdates-almp-prod-001	Azure Database for PostgreSQL flexible server	UAE North
psql-kafka-almp-prod-001	Azure Database for PostgreSQL single server	UAE North
psqlflexianalyticspdns.postgres.database.azure.com	Private DNS zone	Global
psqlflexiprodcoredns.postgres.database.azure.com	Private DNS zone	Global
psqlflexiprodkafkadns.postgres.database.azure.com	Private DNS zone	Global
psqlflexiriderdns.postgres.database.azure.com	Private DNS zone	Global
rediscache-almp-prod-001	Azure Cache for Redis	UAE North
rt-almp-prod-fw-outbound-001	Route table	UAE North
saalmpinfradevopsprod	Storage account	UAE North
snet-prod-almp-aks-syspod-nsg-001	Network security group	UAE North
snet-prod-almp-aksnode-001-nsg	Network security group	UAE North
snet-prod-almp-psql-nsg-001	Network security group	UAE North
stipaasalmpprod01	Storage account	UAE North
subnet-prod-almp-shared-001	Network security group	UAE North
VMALMPMGTPROD001	Virtual machine	UAE North
VMALMPMGTPROD001-nsg	Network security group	UAE North
VMALMPMGTPROD002	Virtual machine	UAE North
vmalmpmgtprod002142	Network Interface	UAE North
vnet-prod-almp-001	Virtual network	UAE North

vnet-prod-almp-001-ip	Public IP address	UAE North
vnetprodalmp001ip852	Public IP address	UAE North

Note : Complete resource information captured under here.

Azure Cloud environment wise resource list - Americana Last Mile Delivery Program - Confluence (atlassian.net)

Disaster Recovery

Business continuity and disaster recovery (BCDR) strategy helps organizations secure data, applications, and workloads during planned or unplanned outages.

Organization and enterprise application workloads have recovery time objective (RTO) and recovery point objective (RPO) requirements.

Category	Systems with HA (Prod within site)	Systems without HA (Non-prod within site)	Disaster Recovery (Across regions)
RPO	RPO is expected to be zero (no data loss)	15 mins	RPO < 5 min*
RTO	RTO in most cases is expected to be less than 120s.	30 mins	RTO – 30 mins *
Availability	99.99% *	99.95%	NA
User Load	Total number of maximum active users :		
	Total number of maximum Concurrent users :		
Service Hours	Operational Service Hours :		
	Peak Usage :		
	Maintenance :		

Effective business continuity and disaster recovery (BCDR) design provides platform-level capabilities that meet these requirements. To design BCDR capabilities, capture platform disaster recovery (DR) requirements.

Disaster Recovery Components

Azure Traffic Manager uses DNS-based routing to load balance incoming traffic across the two regions.

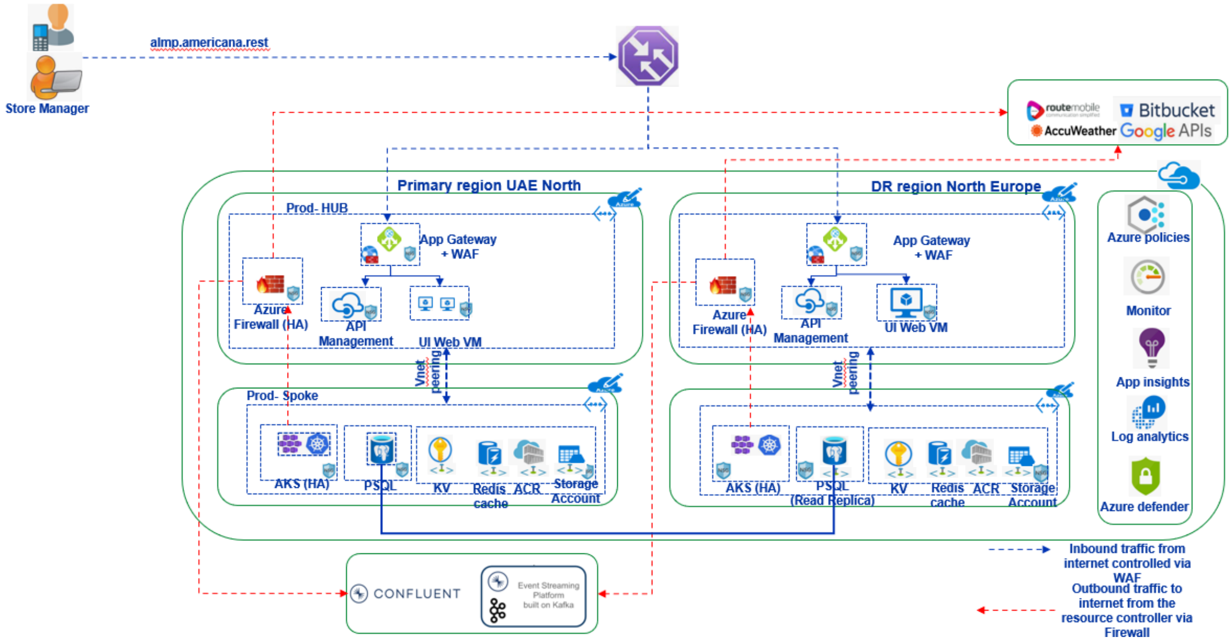
Traffic Manager resolves DNS queries for the application to the public IP addresses of the Application Gateway (AppGW) endpoints.

The public endpoints of the AppGWs serve as the backend endpoints of Traffic Manager. Traffic Manager resolves DNS queries based on the **“priority”** routing methods and the browser connects directly to the endpoint

The “Application Gateways” receive HTTP(S) traffic from the browser and load balance requests across the backend pool of virtual machines (VMs) and API management.

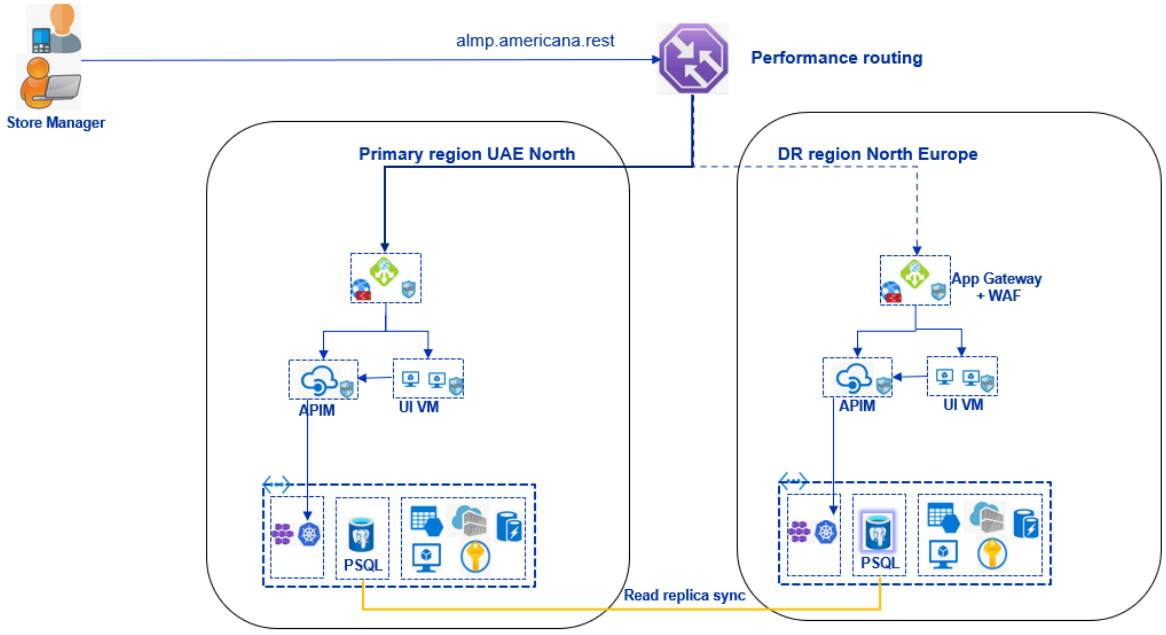
Deploying the “Application Gateways” to all three zones provides zone redundancy. The “Application Gateway” is also distributed traffic across the three zones and it include a Web Application Firewall (WAF) that inspects traffic and protects the application from web exploits and vulnerabilities.

Backend tier business tier processes the user interactions and determines the next steps. It connects the Front end and data tiers. The VMs in the business tier route traffic to the availability group listener of the databases.



The proposed DR plan is to keep the **Active/Passive Hot spare** as a service. The recovery and failover process starts after the event and the traffic will route to the DR region.

Disaster Recovery procedure

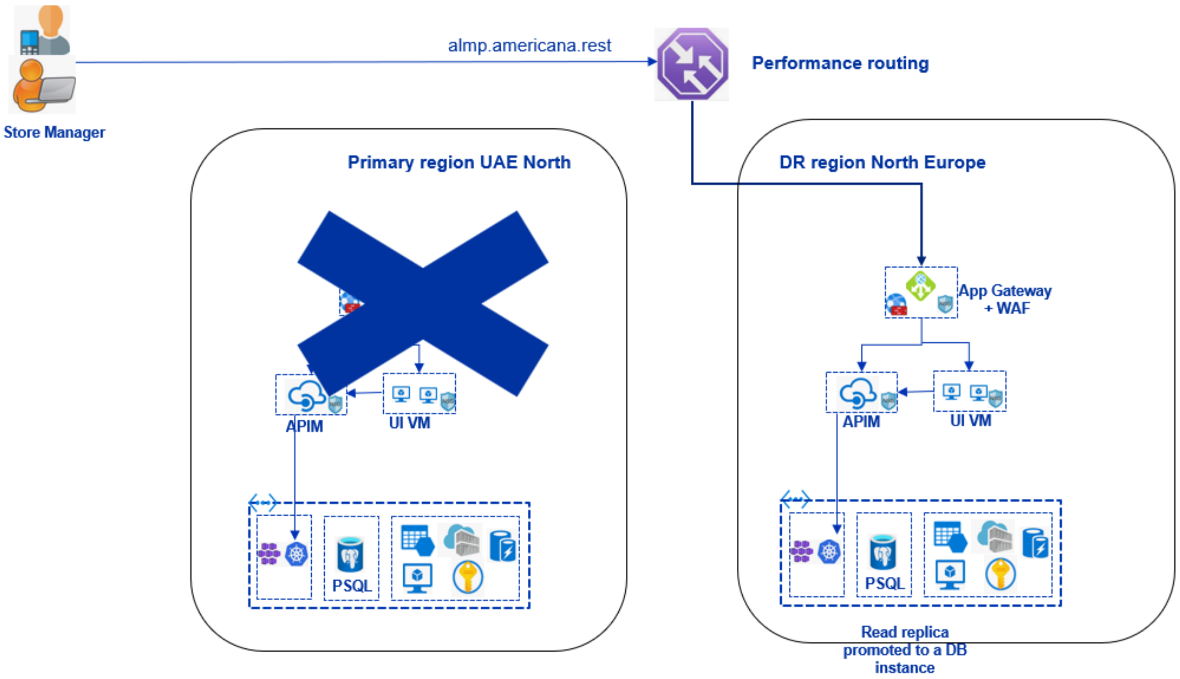


Currently “**North Europe**” considered as a DR region.

During the normal operation

- Traffic Manager directs all the traffic to primary region.
- Application gateway from primary region forwards the traffic to APIM and its further forwards to backend environment.
- Replication established between ACR to replicate the Microservices images, the images hosted
- in primary region will be replicated via ACR and deployed in DR AKS cluster.
- The deployment performed in primary must be deployed in DR AKS to run the identical pods.
- Database replicate across region and “read-replica” in DR replicate keep the “asynchronous copy” of the primary database.

DR Scenario



In the event of region outage,

- Traffic managers probe the failure and direct all the traffic to DR region or initiate the manual failover to DR.
- The inbound from “Traffic manager” direct the traffic to DR application gateway.
- APIM may require to “scale-up” from “Developer” to “Premium.”
- Application gateway further inspect the traffic and forward to APIM
- APIM forwards the request to the relevant “ingress” services hosed in AKS.
- AKS nodes and pods may require to increase dynamically.
- Azure Postgres “read replica” needs to be promoted as a standalone DB to receive a write requests.

Promote “Postgres” SQL read replica to “read/write.”

The promote action causes the replica to apply all the pending logs and promotes the replica to be an independent, standalone read-writeable server. The data in the standalone server is the data that was available on the replica server at the time the replication is stopped. Any subsequent updates at the primary are not propagated to the replica. However, replica server may have accumulated logs that are not applied yet. As part of the promote process, the replica applies all the pending logs before accepting client connections.

replica in a different region from your primary server. Cross-region replication can be helpful for scenarios like disaster recovery planning or bringing data closer to your users.

Disaster Recovery consideration

- RPO/RTO may vary due to the data replication across geographics region.
- The DB failback may take time due to the cross-geo replication constraints.
- APIM SKU needs to be defined on DR, changing SKU during the DR event may impact the RTO.
- The above DR strategy includes only Azure and not includes the DR failover for third party cloud Confluent, Google etc.

DR HUB Environment Components

Resource Name	Resources type	Region
agw-almp-dr-prod-001	Application gateway	North Europe
agw-almp-dr-prod-pip	Public IP address	North Europe
apim-almp-dr-prod-001	API Management service	North Europe
drafwalmphub001	Firewall	North Europe
DRAzureFirewallPolicy	Firewall Policy	North Europe
DRFirewallPublicIP	Public IP address	North Europe
loganalytics-ws-almp-dr-hub-001	Log Analytics workspace	North Europe
MyDRRouteTableRoute	Route table	North Europe
privatelink.blob.core.windows.net	Private DNS zone	Global
vnet-dr-hub-almp-001	Virtual network	North Europe
waf-agw-dr-prod-001	Application Gateway WAF policy	North Europe

DR Spoke Environment Components

Resource Name	Resources type	Region
aks-almp-dr-prod-001	Kubernetes service	North Europe
cralmpdrprod001	Container registry	North Europe
pl-cr-almp-dr-prod-001	Private endpoint	North Europe
pl-cr-almp-dr-prod-001.nic.fbcbadc4-7663-43b0-bce9-18cb2b6f97b3	Network Interface	North Europe
pl-sa-almp-infradevops-dr-prod	Private endpoint	North Europe
pl-sa-almp-infradevops-dr-prod-nic	Network Interface	North Europe
pl-sa-infra-devops-almp-dr-prod	Private endpoint	North Europe
pl-sa-infra-devops-almp-dr-prod-nic	Network Interface	North Europe
privatelink.azurecr.io	Private DNS zone	Global
privatelink.blob.core.windows.net	Private DNS zone	Global
rt-almp-dr-prod-outbound-001	Route table	North Europe
saalmpinfradevopsdrprod	Storage account	UAE North
saalmpinfradevopsdrprodd	Storage account	North Europe
VMALMPMGTDRPROD001	Virtual machine	North Europe

VMALMPMGTDRPROD001-nsg	Network security group	North Europe
vmalmpmgtdrprod001243	Network Interface	North Europe
vmalmpmgtdrprod001746	Network Interface	North Europe
VMALMPMGTDRPROD001nsg603	Network security group	North Europe
vnet-dr-prod-almp-001	Virtual network	North Europe

6. SECURITY/ COMPLIANCE

Security is one of the most important aspects of the architecture. It provides an assurance against deliberate attacks of the valuable data and systems.

Firewall

The hub virtual network acts as a central point of connectivity to many spoke virtual networks. Firewall hosted in HUB network firewall filters out the “Outbound” malicious traffic.

Web Application Firewall (WAF

Provides centralized protection of your web applications from common exploits and vulnerabilities.

Note: The detailed WAF policy will be updated upon security design conformation.

Data encryption

Data encryption at rest is available for services across the software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud model.

All Azure Storage Services enable server-side encryption by default using service-managed keys, which is transparent to the application.

Network security groups

A network-based access control feature using a 5-tuple to make allow or deny decisions NSGs do not provide application layer inspection or authenticated access controls. NSGs will be associated on the subnet level to control traffic moving between subnets within an Azure Virtual Network and traffic between an Azure Virtual Network and the Internet.

Azure Private Link and VNet integration

Azure Private Link enables you to access Azure PaaS Services privately in the virtual network over a private endpoint.

Azure Private Endpoint will be used in all supported PAAS services. A private IP address from the VNet to connect privately and securely to a service powered by Azure Private Link.

7. MONITORING AND GOVERANANCE

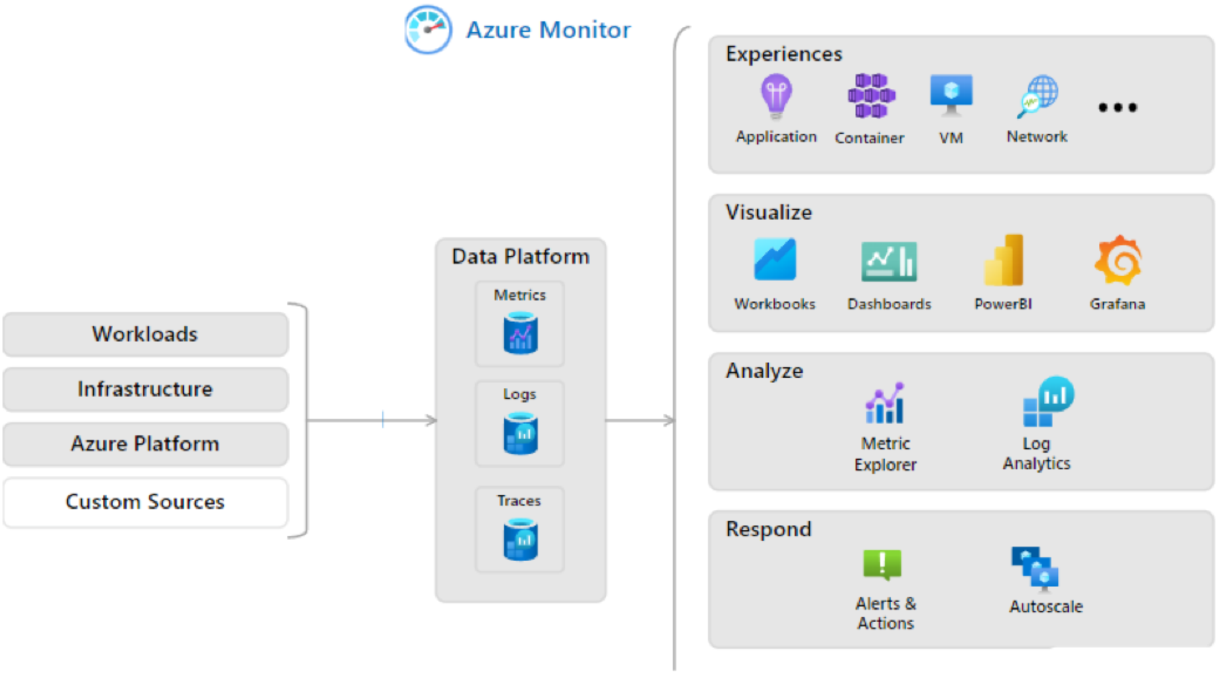
Azure Monitor is Azure's built-in monitoring solution. It unifies application performance, service monitoring, and platform monitoring. The Azure Monitor architecture is designed to consolidate metrics and logs from various resources in Azure and help analyze, visualize, derive insights, and respond to anomalies.

Azure Monitor provides a comprehensive set of services that help cloud administrators keep track of and derive insights about performance, availability, and other telemetry information related to applications.

ALMP workloads will be monitored using Azure native monitoring solution, Azure Monitor. The monitoring solution that will be utilized from Azure is limited to Infrastructure monitoring and application-level monitoring requirement will be added based on a input from application team.

Log analytics collects and store the data from various log sources and allow to query over them using a custom query language. he log will be collected from below sources.

- Azure Monitoring – Metrics (platform) based alerts
- Azure Security Center – Security related data



- **Metrics**: Numeric data collected from the monitored Azure resources. (Metrics will be applied based in discussion with Development team)

- **Logs**: Include more detailed data organized as records, encompassing events, traces, performance information, and more. Logs are used for querying and analysis through tools like Log Analytics.

Governance

Governance provides mechanisms and processes to maintain control over the applications and resources in Azure.

Identity Management

Azure AD is the proposed identity management solution for ALMP. Microsoft Azure Active Directory is an identity and access management cloud solution that provides directory services and identity governance.

Azure resources including azure portal access, authentication and authorization is governed through Azure Active Directory along with “Cyper ark” PAM access.

Azure Policy

Azure policy allows to create, assign, and manage policy definitions to enforce rules for on resources. This feature keeps those resources in compliance with the corporate standards.

RBAC

Azure provides Role Based Access Control, which helps to manage the access to Azure resources, what they can do with those resources, and what areas they have access to. In Americana Azure subscription, the access control of the Cloud resources will be managed and governed based on Resource Groups. The resources will be isolated in respective Resource Groups and provide access to Cloud Operations and Security Operations team based on the guidance given in the below table.

RBACV0.1.xlsx

Resource Provisioning (Azure Devops)

Azure resources are deployed in ALMP subscription using Terraform as IAC and DevOps as build/release manager.

Below are the steps to be performed for any azure resource deployment.

Bitbucket is the source code repository for maintaining terraform scripts.

Env	Repository	Link
NonProd/UAT/Stage repo	almp_nonprod	https://bitbucket.org/almp_dev/almp_nonprod/src/main/
Prod repo	almp_prod	https://bitbucket.org/almp_dev/almp_prod/src/main/
DR Prod repo	almp_dr_prod	https://bitbucket.org/almp_dev/almp_dr_prod/src/main/

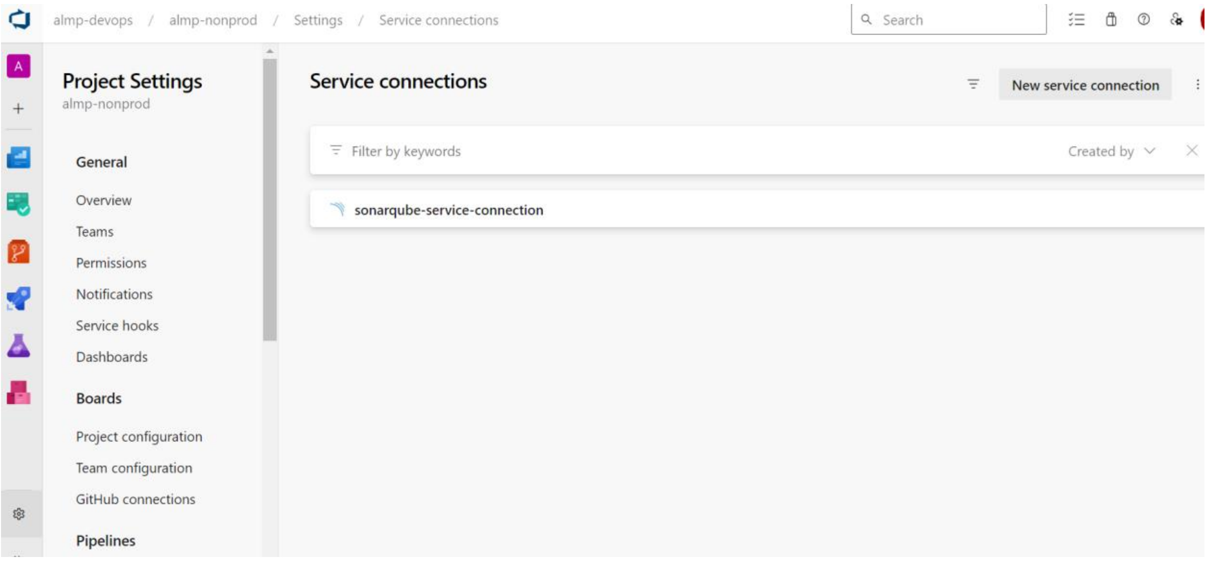
Below are the contents of the repository;

1. **sc.tf** contains the resource modules which is the entry point of code and defines what all configurations that goes in for the specific resource
2. **sc_env.tfvars** contains the variables such as resource name, resource group name etc
3. **sc_parameter.tf** contains the template of each of the variables such as the type of variable, default value etc
4. **azure-pipelines.yml** is the build pipeline script which will be executed by Azure DevOps build pipeline

Azure DevOps is used for maintaining the build/deployment process of resources defined in terraform code. It has three projects namely: almp-dr-prod, almp-prod, almp-nonprod.

Below are the steps to be followed for resource deployment:

1. After the changes and check in process completes in bitbucket the repo management triggers the azure build pipeline instantaneously.
2. Build process creates artifacts which will then be pushed to a temporary container for provision it to release pipeline
3. Release will use this artifact ,validates, awaits peer approval. After peer approval the release pipeline will have to be triggered manually.
4. The release pipeline has four stages :
    a. Terraform package verification
    b. Terraform init
    c. Terraform plan
    d. Terraform apply
5. In each of these stages the parameters viz. artifact location, storage account details where the template will be stored are set
6. In addition, the terraform plan and terraform apply stages have a field called “AzureRM Provider Service Connection” which defines the environment (subscription) in which the resource needs to be deployed
7. The above said service connection needs to be created before hand in Azure DevOps project settings as shown below, also required permissions for service connection needs to be set



The below tables describe project and pipeline details:

DevOps Project	Env	Build Pipeline Name	Release Pipeline Name
almp-dr-prod	DR Prod	almp_dev. almp_dr_prod	Terraform_Deploy_DR_Prod
almp-prod	Prod	almp_dev. almp_prod	Terraform_Deploy_Prod
almp-nonprod	Non Prod	almp_dev. almp_nonprod	Terraform_Deploy_DevEnv
almp-nonprod	UAT	almp_dev. almp_nonprod	Terraform_Deploy_UatEnv
almp-nonprod	Stage	almp_dev. Almp_nonprod	Terraform_Deploy_Stage

8. RESOURCES

AMLP Components list

ALMD-Components
%20V%200.8.xlsx

Infra Queries

Americana-Infra%20
queries%20V0.3.xlsx