Design Document

Low-level Design Document

RCL Foods



Table of Contents

[1. Executive Summary 5](#_Toc201052029)

[1.1. Overview 5](#_Toc201052030)

[2. Wave 1: Landing Zone 2](#_Toc201052031)

[2.1. High-level Design 2](#_Toc201052032)

[2.2. Identity and Access Management 2](#_Toc201052033)

[2.3. Subscription Details 4](#_Toc201052034)

[2.4. Resource Management 4](#_Toc201052035)

[2.5. Networking 5](#_Toc201052036)

[2.6. Governance 4](#_Toc201052037)

[Low-level Design Plan Acceptance 7](#_Toc201052038)

List of Tables

[Table 1: Azure Entra ID 3](#_Toc201052039)

[Table 2: Recommended RBAC Roles 3](#_Toc201052040)

[Table 3: Azure Entra ID Assignments 4](#_Toc201052041)

[Table 4: Conditional Access Policies 4](#_Toc201052042)

[Table 5: Subscriptions Details 4](#_Toc201052043)

[Table 6: Resource Group 5](#_Toc201052044)

[Table 7: Hub Virtual Network 6](#_Toc201052045)

[Table 8: Route Table - zanrgfwrtp01 – Out-to-Firewall 7](#_Toc201052046)

[Table 9: AzureServiceBus 7](#_Toc201052047)

[Table 10: PowerPlatform-Europe 8](#_Toc201052048)

[Table 11: PowerPlatform-VirtualAgents 8](#_Toc201052049)

[Table 12: ServiceTags-AzPowerBi 8](#_Toc201052050)

[Table 13: ExpressRoute – Virtual Network Gateway 9](#_Toc201052051)

[Table 14: ExpressRoute Circuit 10](#_Toc201052052)

[Table 15: Azure Firewall Policy 11](#_Toc201052053)

[Table 16: Azure Firewall 12](#_Toc201052054)

[Table 17: Network Rules 5](#_Toc201052055)

[Table 18: Application Rules 13](#_Toc201052056)

[Table 19: Application Gateway 3](#_Toc201052057)

[Table 20: Private DNS Zone – Azure Websites 3](#_Toc201052058)

[Table 21: Private DNS Zone – Azure Websites 4](#_Toc201052059)

[Table 22: Network Watcher 4](#_Toc201052060)

[Table 23: Key Vault 5](#_Toc201052061)

[Table 24: Storage Account 6](#_Toc201052062)

[Table 25: Log Analytics Workspace 6](#_Toc201052063)

List of Figures

[Figure 1: Landing Zone 2](#_Toc201052064)

Document Configuration Management

**Document Identification**

|  |  |
| --- | --- |
| Title | Low-level Design Document |
| Document Type | Design |
| File Name | RCLFoods\_low-level\_Design\_V0-01 |
| Version | Version 1.0 |
| Sensitivity Classification |  |
| Document Owner | Indren Maistry/Allen Naidoo |

**Preparation**

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Name | Role / Function | Date |
| Prepared by: | Nickyle Alwar | Technical Architect | 2025/06/09 |
| Approved by: | Donovan Kelly | Principal Technical Architect |  |

**Release**

|  | Date Released | Change Notice | Remarks |
| --- | --- | --- | --- |
| 0.01 | <20yy-Mmm-dd> |  | 1st Draft |
|  |  |  |  |

**Contribution (C) and distribution (D) list**

| Name | C/D | Organisation | Title |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

## Overview

The Low-level design document is outlined to detail all specifications for the Azure deployment. The deployment will be conducted in waves starting with the Landing zone as this is the foundational layer of the environment and moving on from development to production workloads.

# Wave 1: Landing Zone

The first wave of the subscription migration project is to start at the foundational level and create a landing zone environment which is amalgamated from the two existing resource groups, namely:

Following production resource groups will be amalgamated into a new resource group in the MCA PROD subscription in this wave:

* zanrgrgldzp001 (Production Subscription)
* zanrgrgldzp001 (Enterprise MCA - Production)

## High-level Design

This is the high-level diagram illustrating the Landing Zone environment in the new “MCA Prod” subscription:

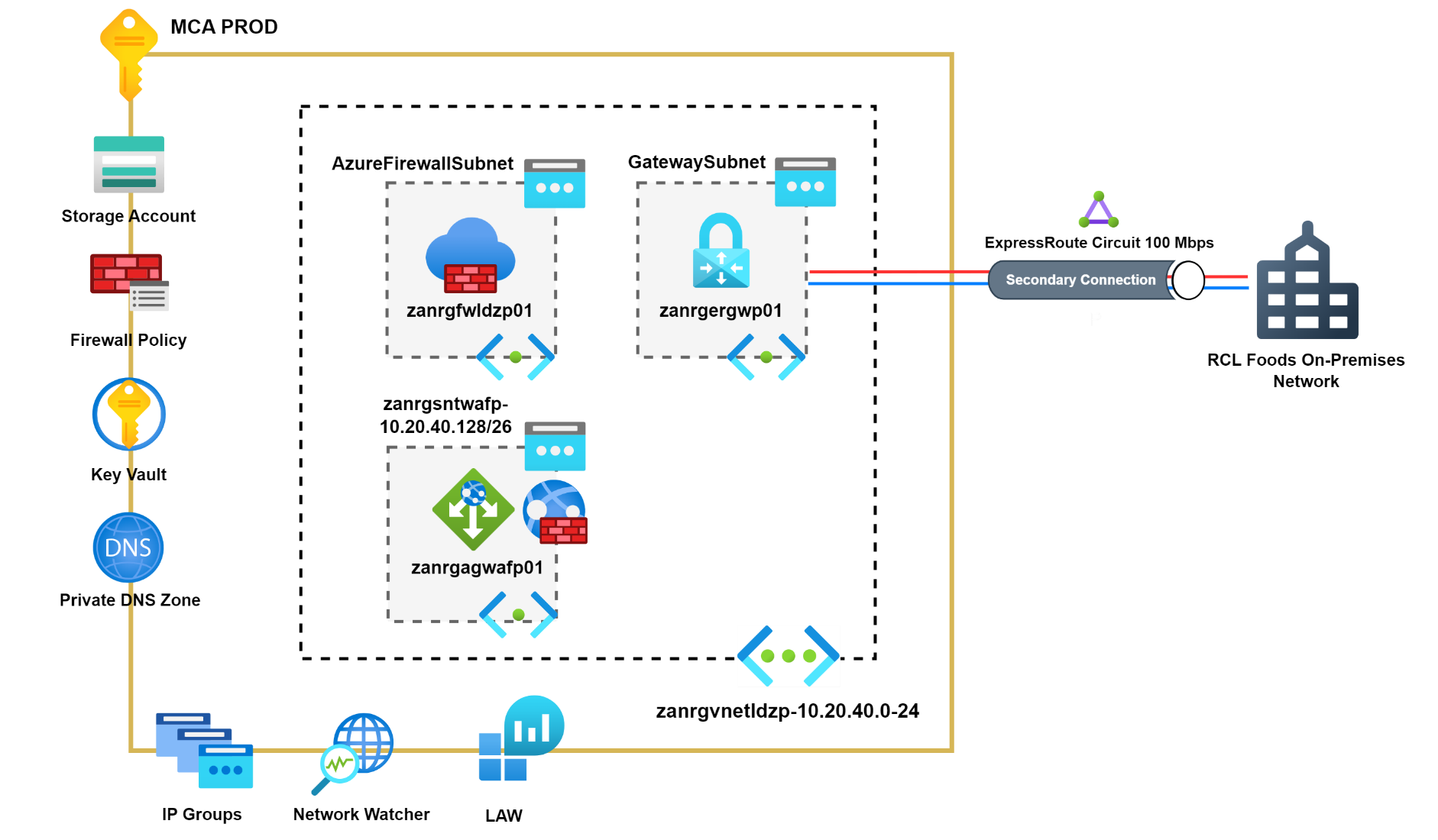


Figure 1: Landing Zone

## Identity and Access Management

This section outlines how to maintain security and compliance in Azure. This will allow RCL Foods to effectively manage identities and control access to resources which is essential to prevent unauthorized access and data breaches.

**Explanation:** Identity and Access Management (IAM) in Azure refers to the set of practices and tools that govern the authentication, authorization, and access control of users and applications to Azure resources.

### Entra ID

This table details RCL Foods Azure Entra ID information and licensing type:

Recommendation to upgrade to **Entra ID Premium P2** for additional security features. Read more here: [Microsoft Entra Plans and Pricing | Microsoft Security](https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing)

| Domain Name | Tenant ID | License |
| --- | --- | --- |
| rclfoods.com | d1da1a04-9e6d-48a9-bb3e-fb293a65ccab | Microsoft Entra ID Free |

Table 1: Azure Entra ID

### Role Based Access Control (RBAC)

The table below depicts the recommended RBAC roles for RCL Foods users, following the principles of least privileges in Azure after the landing zone deployment is complete:

These recommended roles are important to apply to RCL Foods users in the Azure environment because it's important to follow the principle of least privilege, granting only the permissions necessary for the user to perform their tasks. Custom roles are available to be created depending on your specific requirements. Explore more **Azure RBAC roles** here: [Azure built-in roles - Azure RBAC | Microsoft Learn](https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles)

| RBAC Role Name | Description |
| --- | --- |
| Contributor role | The "Contributor" role is a built-in role that grants users a high level of access to resources within a specific scope, such as a subscription, resource group, or individual resource. Users with the Contributor role have the ability to manage and configure resources, but they do not have the ability to manage access to those resources. |
| Reader Role | The "Reader" role grants users read-only access to the Azure resources, which allows them to view configurations, settings, and monitoring data without the ability to make changes. This is a low-risk role that provides good visibility into the environment without posing a significant security risk. |
| Monitoring and Management Role | You could create a custom role that includes read-only access for monitoring purposes, along with some additional permissions to perform basic management tasks. For example, you might add permissions to start/stop virtual machines, view and manage diagnostics settings, and access monitoring logs. This would allow the user to perform necessary management actions without having overly broad access. |
| Security Reader or Security Operator Role | If the user's oversight includes a focus on security and compliance, you could consider assigning them the "Security Reader" or "Security Operator" role. These roles provide access to security-related data, such as Azure Security Center alerts and recommendations, without granting excessive privileges. |

Table 2: Recommended RBAC Roles

### Azure Entra ID (Azure Active Directory) Assignments

| **User** | **Role** | **Description** | **Permissions** | **Scope** |
| --- | --- | --- | --- | --- |
| Nickyle Alwar  Nickyle.Alwar@global.ntt | Contributor | Cloud Technical Architect | Full access | Tenant Root Group |
| Leroy Fourie  leroy.fourie@global.ntt | Lead Engineer |

Table 3: Azure Entra ID Assignments

### Conditional Access Policies

This section details conditional access policies and access controls for target users and groups of users in Azure:

Conditional access policies applied to RCL Foods Azure environment will ensure all users are **verified and authenticated** which helps prevent unauthorised access.

| **Policy Name** | **Target Users/Groups** | **Conditions and Requirements** | **Access Controls** |
| --- | --- | --- | --- |
| MFA Enforced | All users | Location: Outside company network | Require MFA |
| High-Risk Users | Users flagged as high risk | Risk level: High | Require MFA, review access |

Table 4: Conditional Access Policies

## Subscription Details

This section outlines the subscriptions needed for the Landing Zone deployment:

| Subscription Name | SubscriptionID | TenantID |
| --- | --- | --- |
| **MCA PROD** | 89b4f2f0-5607-48ac-9acc-81f64550dc19 | d1da1a04-9e6d-48a9-bb3e-fb293a65ccab |

Table 5: Subscriptions Details

## Resource Management

The following outlines the logical grouping for all the Azure resources to be collectively organised, monitored, and managed:

#### zanrgrgldzp001

**Purpose**: For all shared networking resources in the production environment such as Virtual Network, Subnets, ExpressRoute Circuit, Virtual Network Gateway, Azure Firewall, Public IPs, Route Tables and Network Security Groups.

| Specification | Description |
| --- | --- |
| **Resource Group Name** | zanrgrgldzp001 |
| **Subscription** | MCA PROD |
| **Resource Group Location** | South Africa North |
| **Tags (Added at later stage)** | **Application:** [Empty]  **Application Owner:** [Empty]  **Business Owner:** [Empty]  **Business Unit:** [Empty]  **Company:** [Empty]  **CostCenter:** Add Cost Center Tag  **Criticality:** [Empty]  **Department:** [Empty]  **Division:** [Empty]  **Role:** [Empty] |

Table 6: Resource Group

## Networking

The following outlines all resources needed from a networking perspective for the Landing Zone sites in Azure to be functional, which include Virtual Networking, Subnets, ExpressRoute Circuits, Virtual Network Gateways, Local Network Gateways, Azure Firewalls, Public IPs, Route Tables, Network Security Groups and VNet Peering.

### Virtual Networks

An Azure Virtual Network (VNet) is a software-defined network that provides isolated and secure communication between Azure resources, including virtual machines, databases, and services. It enables users to define private IP address spaces, subnets, and network security groups, ensuring fine-grained control over network topology and traffic flow.

#### Hub Virtual Network

The following details the production hub networks configuration details:

For Wave 1, only network **zanrgvnetldzp-10.20.40.0-24** will be deployed. The other 10.x networks targeted for creation will be deployed at a later wave.

| Specification | Description |
| --- | --- |
| Name | zanrgvnetldzp-10.20.40.0-24 |
| Resource Group | zanrgrgldzp001 |
| Subscription | MCA PROD |
| Region | South Africa North |
| Total Address Space | |  |  |  | | --- | --- | --- | | **Address Space** | **Address Range** | **Address Count** | | 10.20.40.0/24 | 10.20.40.0 to 10.20.40.255 | 256 | |
| Subnet Address Allocation | |  |  |  | | --- | --- | --- | | **Address Space** | **Subnet** | **Description** | | 10.20.40.0/26 | AzureFirewallSubnet | **Azure Firewall Subnet** | | 10.20.40.64/26 | GatewaySubnet | **Expressroute Gateway Subnet** | | 10.20.40.128/26 | zanrgsntwafp-10.20.40.128/26 | **Application Gateway Subnet** | |
| DNS Servers | **Custom:**  183.0.11.36 (Decommission at later stage)  10.20.14.14  10.20.14.15  10.20.14.10  10.20.18.13 |
| Tags (Added at later stage) | **Application:** [Empty]  **Application Owner:** [Empty]  **Business Owner:** [Empty]  **Business Unit:** [Empty]  **Company:** [Empty]  **CostCenter:** Add Cost Center Tag  **Criticality:** [Empty]  **Department:** [Empty]  **Division:** [Empty]  **Role:** [Empty] |

Table 7: Hub Virtual Network

### Route Tables

By default, all subnets inside the same VNet, with the exception of the GatewaySubnet, will share the same route table. Exceptions can be defined based on workload or resources needs.

#### Out-to-Firewall Route Table

More subnet associations will be added at a later stage.

| Specification | Description |
| --- | --- |
| Route Table Name | zanrgfwrtp01 |
| Resource Group | zanrgrgldzp001 |
| Region / Location | South Africa North |
| VNet / Subnet Association | zanrgsntwafp-10.20.40.128/26 |
| Routes | |  |  |  |  | | --- | --- | --- | --- | | **Route Name** | **Address Prefix** | **Next Hop Type** | **Next Hop Address** | | **Out-to-Firewall** | **0.0.0.0/0** | **Virtual Appliance** | 10.20.40.5 | |  |  |  |  | |
| Virtual network gateway route propagation | **Yes** |

Table 8: Route Table - zanrgfwrtp01 – Out-to-Firewall

### IP Groups

This section outlines the IP groups recreated as part of this deployment:

#### AzureServiceBus

|  |  |
| --- | --- |
| **Name** | AzureServiceBus |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| IP Addresses | 13.66.138.80/29  - (284 IPs)  207.46.138.15/32 |
| Tags | **[None]** |

Table 9: AzureServiceBus

#### PowerPlatform-Europe

|  |  |
| --- | --- |
| Name | PowerPlatform-Europe |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| IP Addresses | 52.169.216.196  40.89.131.3  52.174.180.160  52.178.150.68  94.245.91.93  52.174.88.118  40.91.208.65  137.117.161.181  13.69.171.0  13.69.227.208-13.69.227.223  13.69.64.208-13.69.64.223  13.69.71.192-13.69.71.223 |
| Tags | **[None]** |

Table 10: PowerPlatform-Europe

#### PowerPlatform-VirtualAgents

|  |  |
| --- | --- |
| Name | PowerPlatform-VirtualAgents |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| IP Addresses | 52.169.216.196  - (262 IPs)  20.71.81.103 |
| Tags | **[None]** |

Table 11: PowerPlatform-VirtualAgents

#### ServiceTags-AzPowerBi

|  |  |
| --- | --- |
| Name | ServiceTags-AzPowerBi |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| IP Addresses | 13.73.248.4/31  - (220 IPs)  191.238.72.128/28 |
| Tags | **[None]** |

Table 12: ServiceTags-AzPowerBi

### Virtual Network Peering

Added in the later waves, stipulated in the migration plan.

### Virtual Network Gateway (ExpressRoute)

This section outlines the virtual network gateway for the ExpressRoute circuit connection:

| Specification | Description |
| --- | --- |
| Name | zanrgergwp01 |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| SKU | Standard |
| Virtual network | zanrgvnetldzp-10.20.40.0-24 |
| Subnet | GatewaySubnet (10.20.40.64/26) |
| Gateway type | ExpressRoute |
| Public IP address | Name: zanrgergwpip01 (New)  IP Address: TBC  SKU: Standard  Tier: Regional  Assignment: Dynamic |
| Tags (Added at later stage) | **Application:** [Empty]  **Application Owner:** [Empty]  **Business Owner:** [Empty]  **Business Unit:** [Empty]  **Company:** [Empty]  **CostCenter:** Add Cost Center Tag  **Criticality:** [Empty]  **Department:** [Empty]  **Division:** [Empty]  **Role:** [Empty] |

Table 13: ExpressRoute – Virtual Network Gateway

### ExpressRoute Circuits

This section outlines the specifications for the Azure ExpressRoute Circuits to be deployed into the Landing Zone environment.

#### ExpressRoute Circuit

| Specification | Description |
| --- | --- |
| Name | zanrgercp01 |
| Provider | Internet Solutions (IS) – CloudConnect |
| Type | 100 Mbps |
| Billing Model | Unlimited |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| SKU | Premium |
| Virtual network | zanrgvnetldzp-10.20.40.0-24 |
| Peering Location | South Africa North |
| Peering Type | Azure private |
| Tags | **[None]** |

Table 14: ExpressRoute Circuit

### Azure Firewall Policy

This section outlines the specifications for the Azure Policy Firewalls will be created to define the firewall rulesets

The Azure Firewall policy will be recreated, and the rules will be exported to the new policy service.

| Specification | Description |
| --- | --- |
| Name | FirewallPolicy |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| Policy Tier | Standard |
| DNS Settings | Enabled  DNS Servers: Default (Azure-provided)  DNS Proxy: Enabled |
| TLS Inspection | Disabled |
| Rules | * **DNAT rules:** 0 rules in 0 collections * **Network rules:** 41 rules in 15 collections * **Application rules:** 11 rules in 10 collections |
| IDPS | Disabled |
| Threat Intelligence | Alert and Deny |
| Tags | **[None]** |

Table 15: Azure Firewall Policy

### Azure Firewall

This section outlines the specifications for the Azure Firewalls to be deployed into the Landing Zone environment:

The Azure Firewall policy will be recreated. Premium SKU will be used for this Firewall.

| Specification | Description |
| --- | --- |
| Name | zanrgfwldzp01 |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region | South Africa North |
| SKU | Premium |
| Parent Policy Name | FirewallPolicy |
| Virtual network | zanrgvnetldzp-10.20.40.0-24 |
| Subnet | AzureFirewallSubnet (10.20.40.0/26) |
| Private IP | 10.20.40.4 |
| Public IP address | * Name: zanrgfwpip001 (New) * IP Address: TBC * SKU: Standard * Tier: Regional * Assignment: Static |
| Rules | * DNAT rules: 0 rules in 0 collections * Network rules: 41 rules in 15 collections * Application rules: 11 rules in 10 collections |
| Tags | **[None]** |

Table 16: Azure Firewall

### Azure Firewall Rules

The section outlines the Azure firewall DNAT, Network and Application Rules:

#### DNAT Rules

No rules in place for DNAT.

#### Network Rules

| Collection Name | Priority | Action | Rule Name | Source Addresses | Destination Addresses | Destination Ports | Protocols |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Net-Allow-Jbx-2-Dcs | 201 | Allow | Allow-Rdp-Dcs | 181.0.3.4 | 181.0.2.4 | 3389 | TCP |
| Net-Allow-Jbx-2-DevSql | 202 | Allow | Allow-Rdp-DevSql | 181.0.3.4 | 182.0.1.4 | 3389 | TCP |
| Net-Deny-182.0-to-181.0.2.x | 210 | Deny | Deny-182.0-to181.0.2 | 182.0.0.0/16 | 181.0.2.0/24 | \* | Any |
| Net-Deny-182.0-to-181.0.2.x | 210 | Deny | Deny-182.0-to181.0.10 | 182.0.0.0/16 | 181.0.10.0/24 | \* | Any |
| Net-Deny-Port | 211 | Deny | Deby-RPC-and-SharePort | \* | \* | 135, 136, 137, 138, 138, 445 | TCP, UDP, ICMP, Any |
| Net-Allow-RPA-AzServiceBus | 205 | Allow | Allow-RPA-AzServiceBus | 183.0.11.68 | AzureServiceBus, ServiceTags-AzPowerBi, PowerPlatform-VirtualAgents | 80, 443, 5671-5672, 9350-9354 | TCP |
| Net-Allow-Peering | 100 | Allow | NewProd>OldDev | 183.0.0.0/16 | 182.0.0.0/16 | \* | Any |
| Net-Allow-Peering | 100 | Allow | NewProd>NewDev | 183.0.0.0/16 | 184.0.0.0/16 | \* | Any |
| Net-Allow-Peering | 100 | Allow | NewDev>OldDev | 184.0.0.0/16 | 182.0.0.0/16 | \* | Any |
| Net-Allow-Peering | 100 | Allow | OldDev>NewDev | 182.0.0.0/16 | 184.0.0.0/16 | \* | Any |
| Net-Allow-Peering | 100 | Allow | OldDev>NewProd | 182.0.0.0/16 | 183.0.0.0/16 | \* | Any |
| Net-Allow-Peering | 100 | Allow | NewDev>NewProd | 184.0.0.0/16 | 183.0.0.0/16 | \* | Any |
| Net-Allow-DNS | 200 | Allow | Allow-DNS | 181.0.2.4, 184.0.100.4 | 169.63.129.16, 209.244.0.3, 209.244.0.4 | 53 | UDP |
| Net-Allow-DNS | 200 | Allow | Allow-DNS-Jbox | 181.0.3.4 | 169.63.129.16, 209.244.0.3, 209.244.0.4 | 53 | UDP |
| Net-Allow-DNS | 200 | Allow | Allow-DNS-Dev-DataBricks | 182.0.0.0/16 | 169.63.129.16, 209.244.0.3, 209.244.0.4 | 53 | UDP |
| Net-Allow-Zanrgvmbaip01 | 101 | Allow | Bidvest Dev Mgmt | 181.0.10.5 | 154.66.197.165 | 1433 | TCP |
| Net-Allow-Zanrgvmbaip01 | 101 | Allow | Bidvest Temp | 181.0.10.5 | 102.37.99.148 | 1433 | TCP |
| Net-Allow-Zanrgvmbaip01 | 101 | Allow | Bidvest Temp Orig | 181.0.10.5 | 154.66.197.184 | 1433 | TCP |
| Net-Allow-Cybereason | 102 | Allow | CybeReason-Reg | \* | manedrover-r.cybereason.net | 443, 8443 | TCP |
| Net-Allow-Cybereason | 102 | Allow | CybeReason 1 | \* | manedrover-1-t.cybereason.net | 443, 8443 | TCP |
| Net-Allow-Cybereason | 102 | Allow | CybeReason 2 | \* | manedrover-2-t.cybereason.net | 443, 8443 | TCP |
| Net-Allow-Cybereason | 102 | Allow | CybeReason 3 | \* | manedrover-3-t.cybereason.net | 443, 8443 | TCP |
| Allow-KMS | 103 | Allow | KMS | 181.0.0.0/16, 182.0.0.0/16, 183.0.0.0/16, 184.0.0.0/16 | 20.118.99.224, 40.83.235.53, 23.102.135.246 | 1688 | TCP |
| Net-Allow-10.20-OnPrem | 204 | Allow | 10.20-OnPrem | 181.0.3.4 | 10.20.0.0/24 | \* | Any, ICMP, UDP, TCP |
| DC-PasswordProtectionAgent | 104 | Allow | Permitted URLs | 183.0.11.36 | login.microsoftonline.com, enterpriseregistration.windows.net, autoupdate.msappproxy.net, office.com | 443 | TCP |
| Net-Allow-CustomerSpend | 105 | Allow | 1Ai | 183.0.12.84, 183.0.12.85, 184.0.11.244 | 1ai.database.windows.net | 1433 | TCP |
| Net-Allow-CustomerSpend | 105 | Allow | Azure Services | 184.0.11.244, 183.0.12.84, 183.0.12.85 | AzureMonitor, AzureCloud, Sql, Sql.SouthAfricaNorth, Storage, Storage.SouthAfricaNorth | \* | TCP, UDP, Any, ICMP |
| Net-Allow-Internet | 203 | Allow | Allow-Dcs-Internet | 181.0.2.4, 183.0.2.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-DevSql-Internet | 182.0.1.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-Jbx-Internet | 181.0.3.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-ProdSQL-Internet | 181.0.10.5 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-HarryDev-Internet | 182.0.11.4, 184.0.11.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-HarryProd-Internet | 181.0.11.4, 183.0.11.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-RPA-Internet | 183.0.11.68 | \* | \* | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-DDTest-Inter-Temp | 183.0.100.4, 184.0.100.4 | \* | 80, 8080, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-PBIGW-Prod | 183.0.10.5 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-PBIGW-Dev | 184.0.1.4 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-MDR-Internet | 183.0.12.68, 183.0.12.69 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-CSPProd-Internet | 183.0.12.84, 183.0.12.85 | \* | 80, 443 | TCP |
| Net-Allow-Internet | 203 | Allow | Allow-CSPDev-Internet | 184.0.11.244 | \* | 80, 443 | TCP |
| Net-Allow-DCs-AzureServices | 106 | Allow | Azure | 183.0.11.36 | AzureMonitor, ApplicationInsightsAvailability, AzurePortal, AzureSecurityCenter, AzureCloud, AzureBackup, AzureResourceManager | 80, 443 | TCP |

Table 17: Network Rules

#### Application Rules

| Collection Name | Priority | Action | Rule Name | Source Addresses | Target FQDNs | FQDN Tags | Protocols |
| --- | --- | --- | --- | --- | --- | --- | --- |
| App-Allow-Google | 200 | Allow | Allow-Google | 181.0.2.4 | www.google.com |  | Http:80, Https:443 |
| net-azfw-rul-application-allow-http-Common | 203 | Allow | Allow-RPA-Common | 183.0.11.68 | \*.aadrm.com, \*.acompli.net, \*.appex.bing.com, \*.appex-rf.msn.com, \*.aria.microsoft.com, \*.assets-yammer.com, \*.azure-apim.net, \*.azureedge.net, \*.azurerms.com, \*.blob.core.windows.net, \*.cdn.office.net, \*.cloudapp.net, \*.compliance.microsoft.com, \*.config.office.net, \*.cortana.ai, \*.entrust.net, \*.events.data.microsoft.com, \*.flow.microsoft.com, \*.geotrust.com, \*.helpshift.com, \*.hip.live.com, \*.hockeyapp.net, \*.informationprotection.azure.com, \*.itunes.apple.com, \*.keydelivery.mediaservices.windows.net, \*.localytics.com, \*.manage.microsoft.com, \*.media.azure.net, \*.microsoft.com, \*.microsoftonline.com, \*.microsoftonline-p.com, \*.microsoftstream.com, \*.microsoftusercontent.com, \*.msauth.net, \*.msauthimages.net, \*.msecnd.net, \*.msftauth.net, \*.msftauthimages.net, \*.msftidentity.com, \*.msidentity.com, \*.msocdn.com, \*.o365weve.com, \*.office.com, \*.office.net, \*.office365.com, \*.officeapps.live.com, \*.officeconfig.msocdn.com, \*.omniroot.com, \*.onenote.com, \*.online.office.com, \*.onmicrosoft.com, \*.outlookmobile.com, \*.phonefactor.net, \*.portal.cloudappsecurity.com, \*.powerapps.com, \*.protection.office.com, \*.public-trust.com, \*.security.microsoft.com, \*.sharepointonline.com, \*.streaming.mediaservices.windows.net, \*.symcb.com, \*.symcd.com, \*.verisign.com, \*.verisign.net, \*.virtualearth.net, \*.yammer.com, \*.yammerusercontent.com, \*cdn.onenote.net, account.activedirectory.windowsazure.com, account.live.com, account.office.net, accounts.accesscontrol.windows.net, accounts.google.com, acompli.helpshift.com, activation.sls.microsoft.com, activity.windows.com, ad.atdmt.com, admin.microsoft.com, adminwebservice.microsoftonline.com, ajax.aspnetcdn.com, ajax.microsoft.com, amp.azure.net, amsglob0cdnstream13.azureedge.net, amsglob0cdnstream14.azureedge.net, analytics.localytics.com, api.dropboxapi.com, api.localytics.com, api.login.yahoo.com, api.meetup.com, api.office.com, api.passwordreset.microsoftonline.com, apis.live.net, app.adjust.com, app.box.com, apps.identrust.com, appsforoffice.microsoft.com, assets.onestore.ms, auth.gfx.ms, autologon.microsoftazuread-sso.com, becws.microsoftonline.com, bit.ly, by.uservoice.com, c.bing.com, c.bing.net, c.live.com, c1.microsoft.com, cacerts.digicert.com, cdn.forms.office.net, cdn.odc.officeapps.live.com, cdn.optimizely.com, cdn.uci.officeapps.live.com, cdnprod.myanalytics.microsoft.com, cert.int-x3.letsencrypt.org, cl2.apple.com, clientconfig.microsoftonline-p.net, companymanager.microsoftonline.com, compliance.microsoft.com, connect.facebook.net, contentstorage.osi.office.net, crl.globalsign.com, crl.globalsign.net, crl.identrust.com, crl.microsoft.com, crl3.digicert.com, crl4.digicert.com, d.docs.live.net, data.flurry.com, dc.applicationinsights.microsoft.com, dc.services.visualstudio.com, device.login.microsoftonline.com, dgps.support.microsoft.com, directory.services.live.com, docs.live.net, docs.microsoft.com, ecn.dev.virtualearth.net, enterpriseregistration.windows.net, en-us.appex-rf.msn.com, eus-www.sway-cdn.com, eus-www.sway-extensions.com, excelbingmap.firstpartyapps.oaspapps.com, firstpartyapps.oaspapps.com, foodanddrink.services.appex.bing.com, forms.microsoft.com, go.microsoft.com, graph.facebook.com, graph.microsoft.com, graph.windows.net, informationprotection.hosting.portal.azure.net, insertmedia.bing.office.net, isrg.trustid.ocsp.identrust.com, login.live.com, login.microsoft.com, login.microsoftonline.com, login.microsoftonline-p.com, login.windows.net, login.windows-ppe.net, logincert.microsoftonline.com, loginex.microsoftonline.com, login-us.microsoftonline.com, m.facebook.com, mail.google.com, management.azure.com, mem.gfx.ms, mscrl.microsoft.com, msdn.microsoft.com, myanalytics.microsoft.com, myanalytics-gcc.microsoft.com, nexus.microsoftonline-p.com, nps.onyx.azure.net, o15.officeredir.microsoft.com, ocos-office365-s2s.msedge.net, ocsp.digicert.com, ocsp.globalsign.com, ocsp.int-x3.letsencrypt.org, ocsp.msocsp.com, ocsp2.globalsign.com, ocspx.digicert.com, office.live.com, office.microsoft.com, office15client.microsoft.com, office365servicehealthcommunications.cloudapp.net, officeapps.live.com, officecdn.microsoft.com, officecdn.microsoft.com.edgesuite.net, officeclient.microsoft.com, officepreviewredir.microsoft.com, officeredir.microsoft.com, officespeech.platform.bing.com, omextemplates.content.office.net, outlook.uservoice.com, p100-sandbox.itunes.apple.com, partnerservices.getmicrosoftkey.com, passwordreset.microsoftonline.com, peoplegraph.firstpartyapps.oaspapps.com, platform.linkedin.com, play.google.com, policykeyservice.dc.ad.msft.net, prod.firstpartyapps.oaspapps.com.akadns.net, prod.msocdn.com, protection.office.com, provisioningapi.microsoftonline.com, r.office.microsoft.com, rink.hockeyapp.net, roaming.officeapps.live.com, s.ytimg.com, s0.assets-yammer.com, sas.office.microsoft.com, sdk.hockeyapp.net, secure.aadcdn.microsoftonline-p.com, secure.globalsign.com, secure.meetup.com, security.microsoft.com, shellprod.msocdn.com, signup.live.com, signup.microsoft.com, social.yahooapis.com, staffhub.ms, staffhub.uservoice.com, staffhubweb.azureedge.net, suite.office.net, support.content.office.net, support.microsoft.com, support.office.com, sway.com, technet.microsoft.com, telemetryservice.firstpartyapps.oaspapps.com, testconnectivity.microsoft.com, tse1.mm.bing.net, videocontent.osi.office.net, videoplayercdn.osi.office.net, view.atdmt.com, vortex.data.microsoft.com, watson.microsoft.com, watson.telemetry.microsoft.com, weather.tile.appex.bing.com, web.localytics.com, webanalytics.localytics.com, wikipedia.firstpartyapps.oaspapps.com, workplaceanalytics.cdn.office.net, wus-firstpartyapps.oaspapps.com, wus-www.sway-cdn.com, wus-www.sway-extensions.com, www.acompli.com, www.bing.com, www.digicert.com, www.dropbox.com, www.evernote.com, www.google-analytics.com, www.googleapis.com, www.microsoft.com, www.onedrive.com, www.outlook.com, www.sway.com, www.youtube.com |  | Http:80, Https:443 |
| App-Allow-RPA | 204 | Allow | Allow-RPA-MSFTNCSI | 183.0.11.68 | \*.msftncsi.com, \*.analysis.windows.net, \*.login.windows.net, \*.servicebus.windows.net, \*.frontend.clouddatahub.net, \*.core.windows.net, login.microsoftonline.com |  | Http:80, Https:443 |
| App-Allow-Qualys | 206 | Allow | Qualys | \* | qagpublic.qg3.apps.qualys.com, qagpublic.qg2.apps.qualys.eu |  | Https:443 |
| App-Allow-Cybereason | 205 | Allow | Cybereason | \* | \*.cybereason.net, manedrover.owl-recoveries.com, manedrover-r.cybereason.net, manedrover-1-t.cybereason.net, manedrover-2-t.cybereason.net, manedrover-3-t.cybereason.net |  | Https:443, Https:8443 |
| App-Allow-EdgeUpdates | 207 | Allow | Allow-EdgeUpdates | \* | msedge.api.cdp.microsoft.com, edge.microsoft.com, \*.dl.delivery.mp.microsoft.com, config.edge.skype.com, \*.do.dsp.mp.microsoft.com, edge-enterprise.activity.windows.com, edge.activity.windows.com, api.aadrm.com |  | Https:443, Http:80 |
| App-Allow-AzureServices | 201 | Allow | OMS | 181.0.0.0/16, 182.0.0.0/16, 183.0.0.0/16, 184.0.0.0/16 | \*.ods.opinsights.azure.com, \*.oms.opinsights.azure.com, \*.azure-automation.net, \*.blob.core.windows.net |  | Https:443 |
| App-Allow-AzureServices | 201 | Allow | Allow-AzureServices | 181.0.2.0/24, 181.0.3.0/27, 181.0.10.0/26, 183.0.0.0/16, 184.0.0.0/16 |  | MicrosoftActiveProtectionService, WindowsDiagnostics, WindowsUpdate, AppServiceEnvironment, HDInsight, AzureBackup | Http:80, Https:443 |
| App-Allow-Shoprite | 202 | Allow | Shoprite | 181.0.11.4, 182.0.11.4, 184.0.11.4, 183.0.11.4 | \*.shopriteholdings.co.za |  | Http:80, Https:443 |
| App-Allow-CSPAA | 208 | Allow | CSP AA BOT | 183.0.12.84, 183.0.12.85, 184.0.11.244 | www.automationanywhere.com, aai-artifacts.my.automationanywhere.digital, apeople.automationanywhere.com, docs.automationanywhere.com, botstore.automationanywhere.com, cdn.pendo.io, app.pendo.io, data.pendo.io, pendo-static-5673999629942784.storage.googleapis.com, \*.google.com, microsoftedge.microsoft.com, addons.mozilla.org, \*.my.automationanywhere.digital |  | Http:80, Https:443 |
| Deny\_immureprech.biz | 209 | Deny | Deny\_immureprech.biz | 183.0.11.36 | immureprech.biz |  | Http:80, Https:443 |
| Table 18: Application Rules | | | | | | |  |

### Application Gateway

This section details Azure load balancing component which will function as a front-end service for incoming requests:

Azure Application Gateway based on **zanrgagwafp01** from Enterprise MCA Production subscription.

| Specification | Description |
| --- | --- |
| Application Gateway Name | zanrgagwafp01 |
| Subscription | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Virtual Network | zanrgvnetldzp-10.20.40.0-24 |
| Subnet | zanrgsntwafp-10.20.40.128/26 |
| Application Gateway Name | zanrgagwafp01 |
| Region | SA North |
| Tier | WAF\_V2 |
| Capacity Type | Manual |
| Instance Count | 2 |
| Availability Zone | N/A |
| HTTP2 | Disabled |
| WAF Policy | |  |  | | --- | --- | | WAF Mode | Prevention | | Inspect Request Body | Yes | | Body Size Max | 128 KB | | File Upload Limit | 100 MB | | Rule Set | OWASP 3.0 | | Advanced Rule Collection | Enabled | |
| Backend Pools | Added at later stage |
| Backend Settings | * SFWBG\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: Siqalo\_Weighbridge) * RCL\_ACTQ\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: ActivityTracker\_QA) * RCL\_ACTD\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: ActivityTracker\_DEV) * RCL\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: ActivityTracker) * RCL\_ROWSQA\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: RowsQA) * RCL\_ROWS\_HTTPS\_Settings (Port: 443, Protocol: Https, Cookie based affinity: Disabled, Custom Probe: Rows) |
| Frontend IP Configuration | **Private:**   * Type: Private * Name: appGwPrivateFrontendIp (new) * Private IP address: 10.20.40.68 * Associated listeners: None   **Public:**   * Name: appGwPublicFrontendIp (new) * IP Address: TBC * SKU: Standard * Tier: Regional * Assignment: Static |
| Listeners | * SFWBG\_HTTP\_Listener * RCL\_RowsQA\_HTTPS\_Listener * RCL\_RowsQA\_HTTP\_Listener * RCL\_Rows\_HTTPS\_Listener * RCL\_Rows\_HTTP\_Listener * SFWBG\_HTTPS\_Listener * RCL\_HTTPS\_Listener * RCL\_HTTP\_Listener * RCL\_ACTQ\_HTTPS\_Listener * RCL\_ACTQ\_HTTP\_Listener * RCL\_ACTD\_HTTP\_Listener * RCL\_ACTD\_HTTPS\_Listener |
| Rules | * Routing\_Rule\_HTTPS * Routing\_Rule\_HTTP * Routing\_Rule\_ACTD\_HTTP * Routing\_Rule\_ACTD\_HTTPS * Routing\_Rule\_SFWBG\_HTTPS * Routing\_Rule\_SFWBG\_HTTP * Routing\_Rule\_ACTQ\_HTTPS * Routing\_Rule\_ACTQ\_HTTP * Routing\_Rule\_RowsQA\_HTTPS * Routing\_Rule\_RowsQA\_HTTP * Routing\_RuleRows\_HTTPS * Routing\_RuleRows\_HTTP |
| Health Probes | * Rows * RowsQA * Https * ActivityTracker\_QA * Siqalo\_Weighbridge * ActivityTracker\_Dev * ActivityTracker |
| Tags | **[None]** |

Table 19: Application Gateway

### Private DNS Zone

This section details private DNS zones as placeholders for upcoming resources:

#### Azure Websites

Private DNS zone will be created at default settings until configured at later stage.

| Specification | Description |
| --- | --- |
| Private DNS Zone Name | privatelink.azurewebsites.net |
| Subscription Name | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region / Location | South Africa North |
| Record Sets | Default at this stage |
| Virtual Network Links | zanrgvnetldzp-10.20.40.0-24 |
| Tags | **[None]** |

Table 20: Private DNS Zone – Azure Websites

#### Database

Private DNS zone will be created at default settings until configured at later stage.

| Specification | Description |
| --- | --- |
| Private DNS Zone Name | privatelink.database.windows.net |
| Subscription Name | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region / Location | South Africa North |
| Record Sets | Default at this stage |
| Virtual Network Links | zanrgvnetldzp-10.20.40.0-24 |
| Tags | **[None]** |

Table 21: Private DNS Zone – Azure Websites

### Network Watcher

| Specification | Description |
| --- | --- |
| Name | NetworkWatcher\_southafricanorth |
| Subscription Name | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region / Location | South Africa North |
| Tags | **[None]** |

Table 22: Network Watcher

## Governance

The following outlines all resources needed from governance perspective which include Azure key Vault, Storage Accounts and Log Analytics Workspace:

### Key Vault

This key vault will be migrated from the **zanrgrgldzp001 (Production Subscription)** resource group to the **zanrgrgldzp001 (MCA PROD)** resource group.

| Specification | Description |
| --- | --- |
| Key Vault Name | zanrgkvp01 |
| Subscription Name | MCA PROD |
| Resource Group | zanrgrgldzp001 |
| Region / Location | South Africa North |
| SKU | Standard |
| Access Policies | |  |  | | --- | --- | | **Specification** | **Configuration** | | **Principal (Unknown/User)** | * 1455d045-8f07-4d69-98df-b23d8be4db04 * Stephan Brand * Wendall-Wayne   Wagenstroom | | **Permissions** | * Key * Secret * Certificate | |
| Network Configuration | Allow public access from all networks |
| Soft Delete | Enabled |
| Purge Protection | Disabled |
| Tags | **[None]** |

Table 23: Key Vault

### Storage Account

This storage account will be migrated from the **zanrgrgldzp001 (Production Subscription)** resource group to the **zanrgrgldzp001 (MCA PROD)** resource group.

|  |  |  |  |
| --- | --- | --- | --- |
| Specification | **Description** | | |
| Storage Account Name | | zanrgrgldzp001guestdiag |
| Subscription Name | | MCA PROD |
| Resource Group Name | | zanrgrgldzp001 |
| Region / Location | | South Africa North |
| Performance | | Standard |
| Account Kind | | Storage (general purpose v1) |
| Replication | | LRS (Locally Redundant Storage) |
| Access Tier | | Cool |
| Network Connectivity | | Private |
| Secure Transfer Required | | Enabled | |
| Tags | | **[None]** |

Table 24: Storage Account

### Log Analytics Workspace

|  |  |  |  |
| --- | --- | --- | --- |
| Specification | **Description** | | |
| Storage Account Name | | LogAnalyticsWorkspace-Prod-ZAN |
| Subscription Name | | MCA PROD |
| Resource Group Name | | zanrgrgldzp001 |
| Region / Location | | South Africa North |
| Pricing Tier | | Pay-as-you-go |
| Access Control Mode | | Use Resource or Workspace Permission |
| Tables | | Alert  AppCenterError  ComputerGroup  InsightsMetrics  Operation  Usage |
| Network Isolation | | Ingestion access: Enabled from all networks  Query access: Enabled from all networks |
| Tags | | **[None]** |

Table 25: Log Analytics Workspace

# Low-level Design Plan Acceptance

Having carefully reviewed the proposed Low-level design document (Version 1.0), **RCL Foods** hereby acknowledge and fully accept the outlined specification, configurations and responsibilities for the creation of the Azure resources. This acceptance signifies our agreement to proceed with the migration as detailed herein.

|  |
| --- |
| RCL Foods Representative |
|  |
| **Signature** |
|  |
| **Print Name and Title** |
|  |
| **Date** |