**Azure Monitor, Insights and Alerting Combined Low-Level Design**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Daniel Howarth |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| **Template Version** | Created from Template 2024.01 |
| **Title** | **Azure Monitor, Insights and Alerting Low-Level Design Document** |
| **File Name** | **Azure Monitor, Insights and Alerting Low-Level Design Document** |
| **Version** | 1.0 |
| **Status** | Review |
| **Release Date** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preparation |  |  | |  | |
| **Prepared** | Arshdeep Singh |  | |  | |
| **Authorised** | Stewart Edwards | |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 26/04/2024 |

Table of Contents

[1. Architecture 4](#_Toc167703996)

[1.1 Solution Diagram for Azure Monitor 4](#_Toc167703997)

[1.2 Solution Diagram for Azure Alerts 4](#_Toc167703998)

[5.1 Azure Alert Implementation 5](#_Toc167703999)

[5.2 Azure Monitor Logs Implementation 5](#_Toc167704000)

[5.3 Azure Service Health Implementation 5](#_Toc167704001)

[5.4 Azure Monitor Workbooks Implementation 6](#_Toc167704002)

[5.5 Azure Activity Log Implementation 6](#_Toc167704003)

[5.6 Azure Resource Health Alerts Implementation 6](#_Toc167704004)

[1.7 Configure Metric Alerts 6](#_Toc167704005)

[2. Configuration Templates for Azure Alerts: - 7](#_Toc167704006)

[2.1 Azure Monitor Baseline Alerts: - 7](#_Toc167704007)

[2.2 Service Health Alert Settings 7](#_Toc167704008)

[2.3 Resource Health Alert Settings 9](#_Toc167704009)

[2.4 Microsoft Entra Alert Settings 12](#_Toc167704010)

[2.5 Metric Alert Settings 12](#_Toc167704011)

[2.5.1 Azure Application Gateway 12](#_Toc167704012)

[2.5.2 Azure Virtual Machines 13](#_Toc167704013)

[2.5.3 Storage Accounts 15](#_Toc167704014)

[2.5.4 Log Analytics 16](#_Toc167704015)

# Architecture

## Solution Diagram for Azure Monitor

A computer screen shot of a diagram

Description automatically generated

## Solution Diagram for Azure Alerts

**A screenshot of a computer

Description automatically generated**

# 5.1 Azure Alert Implementation

**Action Groups Setup:**

Create below Action Groups at each Landing Zone Level:

1. Infrastructure Alert Group for Infrastructure Operations with Email notification.

2. Application Alert Group for Application Operations with Email notification.

3. Security Alert Group for Security Operations with Email notification.

4. Landing Zone Cost Alert for Platform Owner and Application Owner with Email notification.

5. Network Alert group for Network Operations with Email notifications.

6. IDAM Alert Group for Identity and Access Management Team with same email notifications.

Alert Action Groups details as below:-

ag-infra-01

ag-network-01

ag-security-01

ag-database-01

**Signal Measures Baseline:**

Set Signal Measures to "All Administrative Operations".

**Alert Rules Configuration:**

Metric alert rules for Availability, Performance, and Security.

Event Level selected for "Warning", "Error", "Critical", "Informational" for resource level alerts.

All Event Status (Failed, Started, succeeded) selected for resource level alerts.

# 5.2 Azure Monitor Logs Implementation

**Data Collection Rules:**

Set up data log collection rules for monitored Azure resources.

**Application Log Analytics Workspace:**

Create an Application Log Analytics Workspace.

**Alerting & Monitoring Configuration:**

Configure alerting and monitoring based on Logs data.

# 5.3 Azure Service Health Implementation

**Service Health Notifications:**

* Create Azure Services Health notifications for Planned Maintenance, Health, and Security Advisories for Australia East and Australia Southeast regions. This need to be done for each subscription.

# 5.4 Azure Monitor Workbooks Implementation

**Default Workbooks Usage:**

* Security Operations team should use default workbooks like Azure Resources Locations, Storage Account Overview, and Key Vault Overview for specific insights analysis via dashboards.

# 5.5 Azure Activity Log Implementation

**Usage for Auditing and Compliance:**

* Use Azure Activity Log for auditing and transfer azure activity log to the log analytics workspace (find the law name).

**Log Transfer to Log Rhythm:**

* Configure central log analytics workspace to forward all Activity Logs in Azure Monitor to be transferred to Log Rhythm for monitoring.

# 5.6 Azure Resource Health Alerts Implementation

* Create Resource Health Alerts for all resource types in each subscription.
* Set alerts to include all future resource groups.

## Configure Metric Alerts

* Configure metric alert rules for major resources.
* Use static thresholds for greater control and specificity.

A screenshot of a computer

Description automatically generated

# Configuration Templates for Azure Alerts: -

## Azure Monitor Baseline Alerts: -

There is industry best practice guidance around key alerts metrics and their thresholds which can be configured as a minimum baseline for the alerts. The idea is to setup the minimum set of alerts and build upon them as needed by various teams.

The AMBA (Azure Monitor baseline alerts) is divided into two main sections:

**Azure Resources:** This section provides guidance for individual Azure resources. For each service, there is a list of key alert metrics and the recommended thresholds. We need to compare these with the list of alerts listed in this document as per the design decision and come up with the total list of baseline alerts that are relevant to AV.

**Patterns / Scenarios:** This section provides guidance for common patterns / scenarios (like Azure Landing Zones), as well as policy definition and initiatives for deploying the alerts in our environment.

[Azure Landing Zones | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/)

[Alerts Details | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/Alerts-Details/) (This section contains the list of alerts that can be deployed as part of ALZ pattern)

[Policy Initiatives | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/Policy-Initiatives/) (This section details the ALZ-Monitor Azure policy initiatives leveraged for deploying the ALZ-Monitor baselines.)

**How to deploy these AMBA:-**

We can use Azure devops pipeline or CLI to deploy these alerts. Guidance around how to deploy these alerts are available under below links.

[Introduction to deploying the ALZ Pattern | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/deploy/Introduction-to-deploying-the-ALZ-Pattern/)

[Deploy with Azure Pipelines | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/deploy/Deploy-with-Azure-Pipelines/)

## Service Health Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Alert | Services | Regions | Event Types | Action Group(s) | Description |
| shar-[subscriptionname]-allresources | All services | Australia East, Australia Southeast,  Global | All | ag-infra-01 | Notifies Infrastructure Operations team of any service health issues on any resource type (Row 4 of Activity Alerts) |
| shar-[subscriptionname]-networkresources | Application Gateway  ASGs  Azure Firewall  Bastion Hosts  Connections  DDoS  Express Routes  Firewall Policies  IP Groups  Load Balancer  Local Network Gateway  NAT Gateways  NICs  Network Manager  NSGs  NVAs  Network Watcher  Public IPs  Private Endpoints  VPN Gateways  Route Filter  Route Table  Virtual Hubs  Virtual Network Gateway  Virtual Network  VWAN | Australia East, Australia Southeast,  Global | All | ag-network-01 | Notifies the Network Operations team of any service health issues on Microsoft.Network resource types (Row 19 of Activity Alerts) |
| shar-[subscriptionname]-securityresources | Activity Logs & Alerts  Advisor  Alerts  Alerts & Metrics  Azure Policy  Defender  Sentinel  Key Vault  Monitor  Purview | Australia East, Australia Southeast, Global | All | ag-security-01 | Notifies the Security Operations team of any service health issues on Security related resource types (Row 6 of Activity alerts) |
| shar-[subscriptionname]-databaseresources | Azure Cosmos DB  Azure Cosmos DB for PostgreSQL  Azure Database for MariaDB  Azure Database for MySQL  Azure Database for MySQL flexible server  Azure Database for PostgreSQL  Azure Database for PostgreSQL flexible server  SQL Database  SQL Managed Instance  SQL Server on Azure VMs  SQL Server Stretch Database  Azure Database Migration Service | Australia East, Australia Southeast, Global | All | ag-database-01 | Notifies the Database Operations team of any service health issues on Database resource types (Row 18 of Activity alerts) |

## Resource Health Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alert | Resource Group | Resource Type | Resource | Event Status | Current Resource Status | Previous Resource Status | Reason Type | Description |
| rhar-[subscriptionname]-allresources | All  Enable “Include all future resource groups” | All | All  Enable “Include all future resources” | All | ag-infra-01 | All | All | Notifies the Infrastructure Operations team of any service health issues on Database resource types (row 2 of Activity alerts) |
| rhar-[subscripname]-networkresources | All  Enable “Include all future resource groups” | Application Gateway  ASGs  Azure Firewall  Bastion Hosts  Connections  DDoS  Express Routes  Firewall Policies  IP Groups  Load Balancer  Local Network Gateway  NAT Gateways  NICs  Network Manager  NSGs  NVAs  Network Watcher  Public IPs  Private Endpoints  VPN Gateways  Route Filter  Route Table  Virtual Hubs  Virtual Network Gateway  Virtual Network  VWAN | Australia East, Australia Southeast,  Global | All | ag-network-01 | All | All | Notifies the Network Operations team of any service health issues on Network resource types (Row 21 of Activity alerts) |
| rhar-[subscriptionname]-securityresources | All  Enable “Include all future resource groups” | Activity Logs & Alerts  Advisor  Alerts  Alerts & Metrics  Azure Policy  Defender  Sentinel  Key Vault  Monitor  Purview | Australia East, Australia Southeast, Global | All | ag-security-01 | All | All | Notifies the Security Operations team of any resource health issues on Security related resource types (Row 22 of Activity alerts) |
| rhar-[subscriptionname]-databaseresources | All  Enable “Include all future resource groups” | Azure Cosmos DB  Azure Cosmos DB for PostgreSQL  Azure Database for MariaDB  Azure Database for MySQL  Azure Database for MySQL flexible server  Azure Database for PostgreSQL  Azure Database for PostgreSQL flexible server  SQL Database  SQL Managed Instance  SQL Server on Azure VMs  SQL Server Stretch Database  Azure Database Migration Service | Australia East, Australia Southeast, Global | All | ag-database-01 | All | All | Notifies the Database Operations team of any resource health issues on Database resource types (Row 23 of activity alerts) |

## Microsoft Entra Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alert | Resource Group | Resource Type | Resource | Event Status | Current Resource Status | Previous Resource Status | Reason Type | Description |
| Microsoft Entra | NA | Microsoft Entra Identities and Groups | All | NA | NA | NA | All | Notifies the IDAM team of any service health issues on Entra resource types (Row 24 of activity alerts) |

## Metric Alert Settings

### Azure Application Gateway

The following alerts should be configured for the Application Gateway to alert for unhealthy backends and failed responses:

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **Unhealthy Host Count Alert Settings** |  |
| Signal name | Unhealthy Host Count |
| Threshold | Static |
| Operator | Greater Than |
| Unit | Count |
| Threshold value | 0 |
| Action Group(s) | ag-network-01  ag-infrastructure-01 |
| Severity | 1 – Error |
| mar-appgateway-unhealthyhost-01 | Alerts the associated action groups when the Unhealthy Host value is greater than 0 |
| **Failed Request Alert Settings** |  |
| Signal name | Failed Request |
| Threshold | Static |
| Operator | Greater Than |
| Unit | Count |
| Threshold value | 0 |
| Action Group(s) | ag-network-01  ag-infrastructure-01 |
| Severity | 2– Warning |
| mar-appgateway-unhealthyhost-01 | Alerts the associated action groups when the failed request value is greater than 0 |

### Azure Virtual Machines

The out of the box settings will be configured for Virtual Machines which include:

* CPU %
* Available memory
* Data Disk IOPS
* OS Disk IOPS
* Network In Total
* Network Out Total
* VmAvailability

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **CPU % Alert 1 Settings** |  |
| Alert Rule Name | mar-vm-cpupercentage-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value greater than | 80% |
| **CPU % Alert 2 Settings** |  |
| Alert Rule Name | mar-vm-cpupercentage-02 |
| Severity | 0 – Critical |
| Threshold Type | Static |
| Value greater than | 90% |
| **Available Memory Alert Settings** |  |
| Alert Rule Name | mar-vm-availablememory-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value less than | 1 GB |
| **Data Disk IOPS Alert Settings** |  |
| Alert Rule Name | mar-vm-datadiskiops-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value consumed greater than | 90% |
| **OS Disk IOPS Alert Settings** |  |
| Alert Rule Name | mar-vm-osdiskiops-01 |
| Severity | 1 – Error |
| Threshold Type | Static |
| Value consumed greater than | 90% |
| **Network In Total Alert Settings** |  |
| Alert Rule Name | mar-vm-networkintotal-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value in greater than | Will vary depending on machine. Select a value 10% higher than average Network In values over time. |
| **Network Out Total Alert Settings** |  |
| Alert Rule Name | mar-vm-networkouttotal-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value in greater than | Will vary depending on machine. Select a value 10% higher than average Network Out values over time. |
| **VM Availability** |  |
| Alert Rule Name | mar-vm-availability-01 |
| Severity | 0 – Critical |
| Threshold Type | Static |
| Value is less than | 1 |
| **Action Group For All Alerts** | ag-infrastucture-01 |

### Storage Accounts

|  |  |
| --- | --- |
| Threshold Type | Static |
| **Availability Alert Settings** |  |
| Alert Rule Name | mar-storageaccount-availability-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Aggregation Type | Average |
| Value in less than | 100% |
| **Used Capacity Alert Settings** |  |
| Alert Rule Name | mar-storageaccount-usedcapacity-01 |
| Severity | 1 – Error |
| Threshold Type | Static |
| Value in greater than | 80% of capacity(selected during deployment) |

### Log Analytics

There are several out of the box alerts available for log analytics:

* When the daily cap limit is reached
* Ingestion rate limit
* Operational issues in the workspace

In the Log Analytics workspace the daily cap has not been set so cannot be configured:

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **Rate Limit Alert** |  |
| Alert Rule Name | mar-loganalytics-ratelimit-01 |
| Severity | 2 – Warning |
| **Operational Issues Alert** |  |
| Alert Rule | mar-loganalytics-operationalissues-01 |
| Severity | 2 - Warning |

|  |  |
| --- | --- |
| Workspace Name | log-prd-auea-mgmt-01 |

AMBA (Azure minimum Baseline Alerts)

The purpose of this project is to focus on monitoring for Azure Landing Zone as a common set of Azure resources/services that are configured in a similar way across organizations. This provided us with a starting point on addressing “What should be monitored in Azure?”

* Express Route Circuits
* Express Route Gateways
* Express Route Ports
* Azure Firewalls
* Application Gateways
* Load balancers
* Virtual Networks
* Virtual Network Gateways
* Log Analytics workspaces
* Private DNS zones
* Azure Key Vaults
* Virtual Machine
* Service health

***Monitoring baselines for the above components are proposed to be deployed leveraging Azure Policy and has been bundled into Azure Policy initiatives for ease of deployment and management.*** In addition to the components mentioned there are also a number of other component alerts included in the repo, but outside any initiatives, or disabled by default. These components are:

* Storage accounts
* Network security groups
* Azure route tables

***In addition to the component specific alerts mentioned above the repo also contains policies for deploying service health alerts by subscription.***