**CORE SERVICE DESIGN:**

**Alerting**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Alerting Core Service Design |
| **File Name** | Ambulance Victoria – Alerting Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 7/03/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 7/03/2024 |

Table of Contents

[1. Overview 5](#_Toc151034051)

[1.1 Purpose and Audience 5](#_Toc151034052)

[1.2 Scope and Key Deliverables 5](#_Toc151034053)

[1.3 Glossary and Definitions 6](#_Toc151034054)

[2. Executive Summary 7](#_Toc151034055)

[3. WAF and Security Control Alignment 7](#_Toc151034056)

[3.1 Reliability 8](#_Toc151034057)

[3.1.1 Overview 8](#_Toc151034058)

[3.1.2 ResourceName Reliability Checklist 8](#_Toc151034059)

[3.2 Cost Optimisation 10](#_Toc151034060)

[3.2.1 Overview 10](#_Toc151034061)

[3.2.2 ResourceName Cost Optimisation Checklist 10](#_Toc151034062)

[3.3 Operational Excellence 11](#_Toc151034063)

[3.3.1 Overview 11](#_Toc151034064)

[3.3.2 ResourceName Operational Excellence Checklist 11](#_Toc151034065)

[3.4 Performance Efficiency 12](#_Toc151034066)

[3.4.1 Overview 12](#_Toc151034067)

[3.4.2 ResourceName Performance Efficiency Checklist 12](#_Toc151034068)

[3.5 Security 13](#_Toc151034069)

[3.5.1 Overview 13](#_Toc151034070)

[3.5.2 ResourceName Security Checklist 13](#_Toc151034071)

[4. Architecture Summary 15](#_Toc151034072)

[4.1 Resource Overview 15](#_Toc151034073)

[4.2 Solution Diagram 15](#_Toc151034074)

[4.3 Design Decisions and Justifications 15](#_Toc151034075)

[4.3.1 Virtual Machine Sizing 15](#_Toc151034076)

[4.3.2 Virtual Machine Disk Tiers 15](#_Toc151034077)

[5. Configuration Templates 16](#_Toc151034078)

Appendix

1. Azure Connector for Ivanti ITSM

# Overview

This document covers the baseline design for the Alerting core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Alerting in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Alerting.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Alerting core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Alerting Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that Reliability, Operational Excellence, and Cost Optimisation were relevant.

For this service the main baseline configurations include:

* Service health alerts will be configured for all resources
* Resource health alerts will be configured for all resources
* Action groups will be defined for:
  + Infrastructure Operations
  + Network Operations
  + Database Operations
  + Security Operations
* Log search alerts are not configured by default

# Resource Cost

The following pricing applies to the varies alert types[[2]](#footnote-3):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alert Type | Free units included | Alert rule price (Monthly) | Time Series Price (Monthly) | Additional cost for metric alert w/ dynamic threshold14 |
| Activity Log Alert | Limited to 100 rules per subscription | N/A | N/A | N/A |
| Native Metrics11, 12 | 10 monitored metric time-series per month13 | N/A | **$0.153** | **$0.153** |
| Log Alert (15 minute frequency) | First time-series is included in the log alert rule | **$0.764** | **$0.077** | N/A |
| Log Alert (10 minute frequency) | First time-series is included in the log alert rule | **$1.528** | **$0.153** | N/A |
| Log Alert (5 minute frequency) | First time-series is included in the log alert rule | **$2.292** | **$0.230** | N/A |
| Log Alert (1 minute frequency) | First time-series is included in the log alert rule | **$4.583** | **$0.459** | N/A |

Table 2: Pricing construct for Azure Alerts

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Alerting Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **R1** | Configure service health alert rules. | Yes | Yes | IaC | At deployment |
| **R2** | Configure resource health alert rules. | Yes | Yes | IaC | At deployment |
| **R3** | Avoid service limits for alert rules that produce large scale notifications. | Yes | No | Governance | Operational – during deployment |

Table 3: WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Alerting Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Keep in mind that activity log alerts, service health alerts, and resource health alerts are free of charge. | Yes | No | N/A | N/A |
| **CO2** | When using log search alerts, minimize log search alert frequency. | Yes | No | Governance | Operational |
| **CO3** | When using metric alerts, minimize the number of resources being monitored. | Yes | No | IaC for recommended services, Governance | At deployment default alerts are deployed  Operationally avoid creating too many metric alerts for extra resources |

Table 4: WAF Cost Optimisation checklist summary

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Alerting Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **OE1** | Use dynamic thresholds in metric alert rules where appropriate. | Yes | Yes | IaC | At deployment |
| **OE2** | Whenever possible, use one alert rule to monitor multiple resources. | Yes | Yes | IaC, Governance | At deployment  Operational – avoid creating rules for each resource |
| **OE3** | To control behavior at scale, use alert processing rules. | Yes | No | IaC | At deployment |
| **OE4** | Use custom properties to enhance diagnostics. | No | No | N/A | N/A |
| **OE5** | Use Logic Apps to customize the notification workflow and integrate with various systems. | Yes | No | Governance | Integrations require additional project work |

Table 5: WAF Operational Excellence checklist summary

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[5]](#footnote-6). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Alerting Performance Efficiency Checklist

There is no guidance for alerting under Performance Efficiency.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

Alerting forms part of the Logging and Threat detection pillar of the Microsoft Security Benchmark. There are no specific controls associated with it, but many resources have specific alert recommendations that, if not covered by their core services design, are covered in this document at a high level.

# Architecture Summary

## Resource Overview

Azure Alerts help detect and address issues with infrastructure and applications with proactive notifications[[7]](#footnote-8). Alerts can be set on any log or metric data on the platform. Alert rules are configured for:

* A specific resource
* A signal and data from the resource
* Certain conditions are met

When the conditions of the rule are met, an alert is triggered. The alert will initiate an associated action group. The alerts are stored for 30 days and deleted after this retention period.

When configuring an alert the following are required:

* **Action groups** – when triggered these can prompt notifications or an automated workflow to let members of the group know an alert is triggered. It can take the following actions:
  + Notification via email to Mailbox, SMS, or push notification
  + Automation runbooks
  + Azure Functions/Logic Apps
  + Secure webhooks/webhooks
  + Event hubs
  + ITSM incidents
* **Alert conditions**
* **User response**
* **Alert processing rules** – can make modifications to triggered alerts as they are being fired

### Types of Alerts

Azure Monitor allows for the following alert types:

* **Metric alerts**
* **Log search alerts**
* Activity log alerts
  + **Service Health alerts**
  + **Resource Health alerts**
* **Smart detection alerts (Application Insights)**

### Critical Alerts

Critical Alerts to be notified to the Action groups using SMS

Metric Alerts are alerts that are configured for specific resource types to fire when a condition of the specific metric is met. For example, when CPU exceeds 80% usage.

Log search alerts are used to monitor resources by using Log Analytics queries to evaluate logs at a set frequency. If the search finds that a condition is met, the alert will fire. This is a more advanced form of alerting that requires specific use cases.

Activity log alerts include Service Health alerts and Resource Health Alerts. Service Health Alerts cover all customers in a region meaning the service has an issue across the entire region. Resource Health alerts are specific to only your tenancy.

Finally, Smart Detection Alerts are a function of Application Insights. After initial set up it takes 24 hours for App Insights to learn the normal performance pattern of your applications. When an anomaly is detected, it will fire an alert. No specific configuration is required for this once App Insights is deployed.

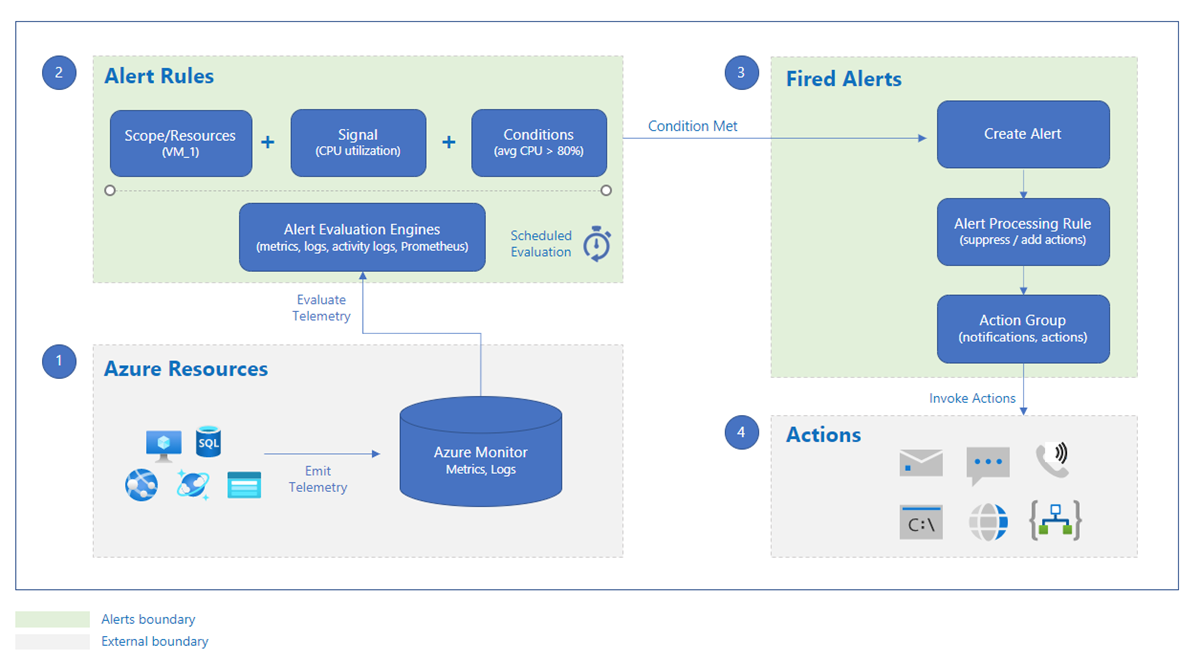
****

Figure 1: Flow of Alerting and Notifications

## RBAC

To set alerts you must have at least Contributor rights on the resource and the following roles to view or manage alerts at the Azure Monitor level:

|  |  |
| --- | --- |
| Role Name | Description |
| Monitoring Reader | People assigned the Monitoring Reader role can view all monitoring data in a subscription but can't modify any resource or edit any settings related to monitoring resources. |
| Monitoring Contributor | People assigned the Monitoring Contributor role can view all monitoring data in a subscription. They can also create or modify monitoring settings, but they can't modify any other resources. |

Table 8: RBAC roles relevant for this core service

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Alerting core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Notifications

**Design Reference:** N/A

**Design Decision:** E-mails will be used for notifications.

**Design Justification:** E-mail notifications are the currently adopted practice for receiving alerts. This will continue to be used as it is a currently adopted practice and requires no change to current processes. Emails will be sent to a Mailbox not to distribution list

### Alert Types

**Design Reference:** N/A

**Design Decision:** Metric, Resource Health, and Service Health alerts will be configured.

**Design Justification:** Metric, Resource Health, and Service Health alerts are broad enough to cover all major resource type requirements, without causing alert fatigue. There are also plenty of out of the box settings that can be created which minimizes the need to do additional customisation work.

### Action Groups

**Design Reference:** N/A

**Design Decision:** Action Groups will be created for the following user groups:

* Infrastructure
* Networking
* DBA
* Security
* IDAM

**Design Justification:** To ensure that teams are appropriately notified for alerts relating to their field, action groups will be created. This will allow the network team to only receive notifications relating to networking alerts as an example.

### Resource health alerts

**Design Reference:** Table 3 – [R2](#_Alerting_Reliability_Checklist)

**Design Decision:** Resource Health alerts will be configured for all resource types.

**Design Justification:** Resource Health alerts are scoped to a subscription and must be re-created on each subscription. They will be set to include all future resource groups in case more are created. All resource types will be covered, but there will also be rules created for function-specific teams such as Networking and Database.

### Service Health Alerts

**Design Reference:** Table 3 – [R1](#_Alerting_Reliability_Checklist)

**Design Decision:** Service Health Alerts will be configured for each subscription.

**Design Justification:** Service Health Alerts cannot span more than one subscription, so they are required to be re-created each time. The alerts for Service Health will be set for all resource types. There will also be rules created for function-specific teams such as Networking and Database.

### Metric Alerts

**Design Reference:** Table 4 – [CO3](#_Alerting_Cost_Optimisation) Table 5 – [OE1](#_Alerting_Operational_Excellence)

**Design Decision:** Metric alert rules will be recommended for major resources including:

* Azure Application Gateway
* Azure Virtual Machines
* Storage Accounts
* Log Analytics Workspace

Static thresholds will be used over Dynamic Thresholds.

**Design Justification:** It is generally not recommended to configure metric alerts for every single service for every metric as this will lead to alert fatigue and will result in major alerts being missed. There are several out of the box recommended alerts for resources such as Virtual Machines that will be enabled by default. The resources mentioned above have their specific recommended metric alerts in the Configuration Templates section.

Any other resources can also have metric alerts enabled as required.

Additionally, Static thresholds will be used as they grant you greater control and allow you to specify exact metrics (e.g. 90%) instead of the inbuilt dynamic thresholds (low, medium, high).

### Log Search Alerts

**Design Reference:** N/A

**Design Decision:** Log search alerts will not be configured as a default.

**Design Justification:** Log search alerts are more advanced and require specific use cases that cannot be met by other standard alerts such as metric or resource health alerts. It is recommended to create these unless necessary as it can lead to alert fatigue alongside all other alerts being created.

# Azure Policies

There are no additional Azure Policies required.

# Configuration Templates

## 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 |
| 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 |
| 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 |
| 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 |

## 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 |
| 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 |
| 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 |
| 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 |

## 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 |

## 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 | [Select value based on storage account expected use] in GB |

### 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 |

# Appendix

## Azure Connector for Ivanti ITSM

It is possible to direct Azure alerts to Ivanti. Please refer to the URL for further information regarding the process.

<https://help.ivanti.com/ht/help/en_US/CLOUD/vNow/Connectors/connector-Azure.htm>

The configuration of directing Azure alerts would not be included as part of IAC code structure.

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-us/pricing/details/monitor/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview [↑](#footnote-ref-8)