**Azure Monitor High-Level Design Document**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | IT |
| **Contact Name** | Daniel Howarth |
| **Email** | Director - ICT Technical Services and Cyber Security |
| **Telephone** | daniel.howarth@ambulance.vic.gov.au |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Business Owner Details | |
| Division | DTS |
| **Contact Name** | Daniel Howarth |
| **Email** | Director - ICT Technical Services and Cyber Security |
| **Telephone** | daniel.howarth@ambulance.vic.gov.au |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| **Template Version** | Created from Template 2024.01 |
| **Title** | **Azure Monitor High-Level Design Document** |
| **File Name** | **Azure Monitor High-Level Design Document** |
| **Version** | 1.0 |
| **Status** | Review |
| **Release Date** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Jeff Chowdhury |  |  |
| **Authorised** | Stewart Edwards |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 15/04/2024 |

Table of Contents

[1. Overview 5](#_Toc164546039)

[1.1 Purpose and Audience 5](#_Toc164546040)

[1.2 Scope and Key Deliverables 6](#_Toc164546041)

[1.3 Out of Scope 6](#_Toc164546042)

[1.4 Glossary 6](#_Toc164546043)

[2. Executive Summary 6](#_Toc164546044)

[3. Architecture 7](#_Toc164546045)

[3.1 Solution Diagram 7](#_Toc164546046)

[3.2 Architecture Deviations 8](#_Toc164546047)

[3.3 SLA 8](#_Toc164546048)

[4. Azure Monitor Cost 8](#_Toc164546049)

[5. Azure Monitor Solution 8](#_Toc164546050)

[5.1 Azure Alert 8](#_Toc164546051)

[5.2 Azure Monitor Logs 9](#_Toc164546052)

[5.3 Azure Service health 9](#_Toc164546053)

[Planned Maintenance 10](#_Toc164546054)

[Health Advisories: 10](#_Toc164546055)

[Security Advisories: 10](#_Toc164546056)

[5.4 Azure Monitor Workbooks 10](#_Toc164546057)

[5.5 Azure Activity Log 10](#_Toc164546058)

[6. Azure Monitor Insights 11](#_Toc164546059)

[6.1 Data Collection Rules 11](#_Toc164546060)

[6.2 Data Collection Rules Automation 12](#_Toc164546061)

[7. Governance 12](#_Toc164546062)

[7.1 Diagnostic Settings 12](#_Toc164546063)

[7.2 Monitor Application with Application Insight 12](#_Toc164546064)

[7.3 Monitor VM with VM Insight 12](#_Toc164546065)

[7.4 Monitor Container with Container Insight 13](#_Toc164546066)

[7.5 Monitor Network with Network Insight 13](#_Toc164546067)

[7.6 Monitor Storage Account with Storage Insight 14](#_Toc164546068)

[7.7 Monitor Key Vault with Key Vault Insight 14](#_Toc164546069)

[8. Operations 15](#_Toc164546070)

[8.1 VM Monitoring Deployment Agent 15](#_Toc164546071)

[8.2 Storage Account Monitoring Enforcement 15](#_Toc164546072)

[8.3 Key Vault Monitoring Deployment Agent 15](#_Toc164546073)

[9. Azure Monitor Access Control 16](#_Toc164546074)

[10. Azure Monitor Security Control 16](#_Toc164546075)

[11. Architecture Acceptance 16](#_Toc164546076)

# Overview

Ambulance Victoria's digital transformation initiative is a strategic Endeavor aimed at modernizing its operations and services through the adoption of digital technologies. As part of this transformation, Ambulance Victoria is evaluating a Datacenter exit strategy, which involves transitioning its IT infrastructure and services away from traditional on-premises datacentres to cloud-based solutions or other modern hosting platforms.

Key Components of the Digital Transformation and Datacenter Exit Strategy:

1. Cloud Adoption
2. Datacenter Exit
3. Infrastructure and Application Modernisation

To facilitate an Enterprise Infrastructure platform to support Ambulance Victoria’s digital transformation, A well architected Azure Tenant is configured that requires the need for enabling Key Azure services like Azure Advisor, Azure Monitor and other Azure platform services.

## Purpose and Audience

This document will provide the proposed design and configuration of Azure Monitor in Ambulance Victoria’s Azure tenancy as a High-Level Design from an architectural perspective.

This document achieves the following:

* + Provides an overview of the configuration items of Azure Monitor
  + Instructs the configuration items that needs to be enabled and configure.
  + Provides a centralized platform for monitoring and managing the performance of Azure Resources
  + Provides a centralized platform for monitoring and managing Azure services health.

This design is intended to meet the following requirements:

* Microsoft Cloud Adoption Framework
* Department of health controls
* Standard monitoring components enablement of every deployable Azure workload.

The audience for this document is those involved in the planning, designing, and implementing of the Databricks 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 design document covers the architecture and configuration of Azure Monitor to the following aspects.

* Azure Monitor Configurations
* Azure Monitor Logs and associated Log analytics workspace
* Workbooks related to Azure Monitor
* Azure Monitor Insights
* Recommendations of IaC templates for Azure Resources with insight capabilities.

## Out of Scope

While Azure Monitor offers extensive capabilities for monitoring various aspects of Azure resources and applications, there are certain items that fall outside its scope. Some of the out-of-scope items for Azure Monitor include:

* Non-Azure Resources
* OS Level Testing
* Code debugging in Azure DevOps
* Application Code monitoring
* End-user experience monitoring

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **VMSS** | Virtual Machine Scale Set |
| **VNet** | Virtual Network |
| **RT** | Route Table |
| **RBAC** | Role Based Access Control |
| **LB** | Load Balancer |
| **AKS** | Azure Kubernetes |
| **IaaS** | Infrastructure as a Service |
| **WAF** | Web Application Firewall |
| **LAW** | Log Analytics Workspace |

# Executive Summary

Azure Monitor is a comprehensive monitoring service provided by Microsoft Azure, designed to help organizations gain insights into the performance and health of their applications, infrastructure, and networks running on the Azure cloud platform. It offers a range of features for monitoring, collecting, analysing, and acting on telemetry data from various sources, including applications, virtual machines, containers, and more.

Azure Monitor key features are:

* Metrics
* Logs
* Alerts
* Dashboards
* Application Insights
* Network Monitoring
* Service Health

Tailored for security & operations engineers, this document should be treated as guiding principal for continual improvement and monitoring of solutions hosted in Azure.

Azure Monitor will allow Ambulance Victoria’s operations team to:

* Effectively Monitor & manage Azure resources and solutions.
* Optimize availability & security.
* Investigate performance related events.
* Provides visibility and insights into access and fine-grained auditing capability.
* Enhance operational efficiency and reliability.

# Architecture

## Solution Diagram

A computer screen shot of a diagram

Description automatically generated

## Architecture Deviations

At this stage, no deviations from standard architecture are required however changes to proposed Architecture deviations will require standard architectural approval process.

## SLA

Azure Monitor itself does not have a dedicated Service Level Agreement (SLA) published by Microsoft. However, Azure services, including those that Azure monitor integrates with, have their own SLAs covering availability, performance, and support response times.

# Azure Monitor Cost

While Azure Monitor itself doesn’t have a cost associated with it, Azure Monitor offers a range of capabilities for monitoring, logging, and analysing telemetry data from various Azure services and resources, which will attract its own pricing model. These costing are explained below:

**Metrics**: Azure Monitor doesn't cost anything for collecting and storing Basic Metrics data but custom metrics or extended data retention.

**Logs**: Azure Monitor Logs collect and analyse log data from Azure resources, applications, and custom sources. This cost is based on the volume of data ingested and stored.

**Alerts**: Alerts based on metrics and log is a basic functionality of Azure Monitor at no additional cost for basic alerting functionality, forwarding alerts to external services like Splunk or AWS workspace has extra cost.

**Application Insights**: Integrated with Azure Monitor, Application Insights provides application performance monitoring (APM) capabilities. Costing is based on volume of telemetry data collected and stored.

**Network Monitoring**: Network monitoring in Azure Monitor shows telemetry of performance and connectivity of virtual networks, VPN gateways, and ExpressRoute circuits. There are no costs associated to network monitoring.

**Service Health**: Azure Monitor provides insights into the health and availability of Azure services at no extra cost.

# Azure Monitor Solution

## Azure Alert

Azure Monitor Alert is a feature within Microsoft Azure that notifies of critical conditions and can take corrective action.

Alert rules can be based on metric or log data. Metric alert rules provide near-real-time alerts based on collected metrics of

* Availability
* Performance
* Security

of your applications and services running on Azure.

Azure Alert has below mandatory dependencies that should be considered before creating alerts.

* Action Groups
* Alert Rules

1. Signal Measure
2. Alert Logics
3. Event Level
4. Status

Design Decision**:** 4 Actions Groups should be setup at each Landing Zone Level shown below.

|  |  |  |
| --- | --- | --- |
| Action Group Name | Security Group | Notification type |
| Infrastructure Alert Group | Infrastructure Operations | Email |
| Application Alert Group | Application Operations | Email |
| Security Alert Group | Security Operations | Email |
| Landing Zone Cost Alert | Platform Owner, Application Owner | Email |

Signal Measures at a baseline should be set to “All Administrative Operations”.

Event Level should be selected for “Warning”, “Error”, “Critical”, “Informational” for only creating alert at the resource level. This is not a mandatory requirement while create the action group.

All Event Status (Failed, Started, succeeded) should be selected when creating a resource level alert. This is not a mandatory requirement while create the action group.

## Azure Monitor Logs

Azure Monitor Logs is a feature of Azure Monitor that collects and organizes log and performance data from monitored Azure resources.

Several features of Azure Monitor store their data in Logs and present this data in various ways to assist in monitoring, performance, and availability of services.

Azure Monitor Logs works with:

* Data log collections Rules
* Application Log Analytics Workspace
* Alerting & Monitoring

## Azure Service health

* Azure Service Health is a feature within Microsoft Azure and available to be accessed from Azure Monitor blade that provides information about the current health status of Azure services in various regions around the world. It keeps Azure
* users informed about any ongoing service incidents, planned maintenance events, and other issues.

Service Health are broken in to 3 Categories:

* Planned Maintenance
* Health Advisories
* Security Advisories

Planned Maintenance:

Azure Service Health Planned Maintenance refers to scheduled maintenance activities performed by Microsoft Azure to ensure the reliability, security, and performance of Azure infrastructure and services.

Health Advisories:

Azure Service Health advisories are notifications and recommendations provided by Microsoft Azure to inform users about issues that may affect the availability & performance of their Azure resources.

Security Advisories:

Azure Service Security Advisories are notifications provided by Microsoft Azure to inform users about security vulnerabilities, threats, or issues that may affect the security posture of their Azure resources and applications.

Design Decision**:**

Azure Services Health notifications must be created for the above 3 categories (Planned Maintenance, Health & Security Advisories) for all Azure Services but for only below regions,

* Australia East
* Australia Southeast

The Alerts configured to use “Infrastructure Alert Group” action group mentioned above.

## Azure Monitor Workbooks

Workbook in Azure Monitor enables users to create interactive, customizable dashboards for visualizing and analysing data from various Azure services and resources.

Design Decision**:**

Security Operations team should be using the default workbooks to analyse specific insights via dashboards.

Below Workbooks are suggested to be used:

* Azure Resources Locations
* Storage Account Overview
* Key Vault Overview

## Azure Activity Log

The Azure Activity Log is a platform-level log service in Microsoft Azure that provides visibility into operations that are being performed on resources in Ambulance Victorias

Azure subscriptions. It records all control-plane events that occur within Azure resources. These details focus on:

Visibility: Visibility into actions and operations (failed & successful) performed in Azure

Granularity: Gives granular information on operation, time, user.

Design Decision**:**

Activity Log is suggested to be used for auditing a compliance reason by the security & infrastructure operation team.

Activity Logs in Azure Monitor is also being transferred to Log Rhythm.

# Azure Monitor Insights

Azure Monitor Insights provides advanced analytics and intelligence capabilities to help Ambulance Victoria gain deep insights into the performance and health of hosted applications and infrastructure.

Azure Monitor Insights have below configurable insights.

* Applications
* Container
* VM
* Network
* SQL
* Key Vault

Design Decision**:**

Above Resource Application insight should be enforced to be configured during deployment of these resources.

## Data Collection Rules

Azure Monitor Data Collection Rules (DCR) allows to collect data from a variety of sources and route it to different destinations for analysis, storage, or further processing.

It provides a flexible and scalable way to gather telemetry data from different Azure services, applications, and virtual machines, and then route that data to Azure Monitor or other destinations such as Azure Storage, Event Hubs, or Log Analytics workspaces.

Design Decision**:**

Below Data sources must be configured for Linux VM Teant wide

* Performance Counters
* Linux Syslog Counters

Below Data sources must be configured for Windows VM Teant wide

* Performance Counters
* Windows Event Log

## Data Collection Rules Automation

Data Collection Rules (DCR) Automation refers to the process of automating the configuration and management of data collection rules within Azure Monitor.

The automation will be achieved via enforcing,

1. VM insights, Container Insights, Network Insights during resource deployment via bicep template
2. Azure Container Insights
3. Azure Network Insights

# Governance

Azure Monitor is mainly aimed at IT infrastructure Operations Team & Security Operations team as it provides a way of monitoring Resources or solutions.

## Diagnostic Settings

Azure Monitor Logs is a feature of Azure Monitor that collects and organizes log and performance data from monitored Azure resources, however one of the core requirements of monitoring Azure Resources of its health and performance is the resource logs itself that must be enabled via resources Diagnostics Settings configuration option.

To capture resource logs the below diagnostics logs must be enabled.

1. All Metric Logs
2. Performance counter Logs via DCR (Data Collection Rules)

## Monitor Application with Application Insight

Azure Monitor Application Insights, a feature of Azure Monitor, excels in Application Performance Management (APM) for live web applications.

Application Insights provides many experiences to enhance the performance, reliability, and quality of your applications.

Application Monitoring requires 2 mandatory configurations.

Design Decision**:**

1. All Metrics and logs must be configured to a central Application Log Analytics Workspaces in the Hub Subscription.
2. Application insight settings must be enabled and configured to the same Application Log Analytics Workspace.

## Monitor VM with VM Insight

Monitoring virtual machines (VMs) with Azure Monitoring Insights involves collecting telemetry data, and then configuring Application Insights to analyse and visualize that data.

VM insights in Azure Monitor will provide:

* Simplified onboarding of the Azure Monitor agent to enable monitoring of a virtual machine guest operating system and workloads.
* Preconfigured data collection rule that collects the most common set of performance counters for Windows and Linux.
* Predefined trending performance charts and workbooks that you can use to analyse core performance metrics from the virtual machine's guest operating system.

Design Decision**:**

Types of Virtual Machines that should monitored by Azure Monitor are

* Azure VM
* Azure VM Scale Sets
* VDI

Below configurations are mandatory for all VM for Monitoring in General.

* Deploy Azure Monitoring Agent
* Configure VM data collection.

## Monitor Container with Container Insight

Container insights of Azure Monitor collects and helps to analyse container logs from

* Azure Kubernetes clusters.
* Azure Arc-enabled Kubernetes clusters

and their components.   
The collected data then can be analysed with a collection of views and prebuilt workbooks.

Container insights support various type container environments.

Design Decision**:**

Container insights must be configured for the most widely used containers, i.e.

* Azure Kubernetes Services (AKS)
* Azure Arc-enabled Kubernetes Cluster
* VMware Tanzu (TKG)

Below configurations are mandatory for all containers for Monitoring in General

* Azure Monitor agent for Linux
* Log Analytics Agent
* Data Collection Rules

## Monitor Network with Network Insight

Azure Monitor Network Insights provides a comprehensive and visual representation through topology, health, and metrics for all deployed network resources, without requiring any configuration. It also provides access to network monitoring capabilities like Connection monitor, NSG flow logs, and Traffic analytics. Additionally, it provides other network diagnostic features.

Network components that should be monitored by Network Insights are:

* Network Health Metrics
* Connectivity
* Traffic Metric

By default, all networking resources are visible in Azure Monitor network insights by simply enabling “All Metrics” of diagnostics settings.

Design Decision**:**

Azure Network Watcher must be deployed for each VNET under the standard service deployment model of an Application Landing Zone.   
Network Watcher will provide below network related tools to further enhance network monitoring and troubleshooting tasks.

* IP flow verify.
* NSG diagnostics
* Next hop
* Effective security rules
* Connection troubleshoots.
* Packet capture
* VPN troubleshoots.

## Monitor Storage Account with Storage Insight

Storage insights is a comprehensive monitoring blade of all Storage accounts in a unified view that shows performance, capacity, and availability metrics.

Storage capacity, and performance can be drilled in two ways:

* View directly from a storage account.
* View from Azure Monitor to see across groups of storage accounts.

Design Decision**:**

To monitor storage accounts associated metrics

* All Metric diagnostics logs should be configured to a central Application Log Analytics Workspace

## Monitor Key Vault with Key Vault Insight

Key Vault insights provides comprehensive monitoring of your key vaults by delivering a unified view of your Key Vault requests, performance, failures, and latency

While the Overview page in the Azure portal for each key vault includes the following metrics on the "Monitoring" tab:

* Total requests
* Average Latency
* Success ratio

Key Vault insight can provide further granular data.

Design Decision**:**

To monitor Key Vault metrics

* All Metric diagnostics logs should be configured to a central Application Log Analytics Workspace

# Operations

## VM Monitoring Deployment Agent

The Azure Monitor agent is implemented as a virtual machine extension, so you can install it using a variety of standard methods including:

* Azure Policy
* Windows Client Installer
* IaC
* VM Insights in Azure Monitor Portal

Design Decision**:**

For Ambulance Victoria, the decision is to follow below process for installing VM Agents

* Install agent via Bicep as part of the VM deployment. (IaC)
* Optionally enforce by policy and user managed identity with condition of “If not exists”.
* At a last resort investigate from VM Insight blade for the missing agent and then install.

## Storage Account Monitoring Enforcement

Storage account diagnostic settings in Azure allow you to configure monitoring for your storage account. This feature enables you to collect various metrics and logs, such as metrics for capacity, ingress, egress, and transactions.

Design Decision**:**

Diagnostics Settings enforcement will be achieved by following:

1. Enforcement of diagnostics settings (Metric, transaction & Storage) via code during deployment
2. Optionally enforce by policy and user managed identity with condition of “If not exists”.
3. At a last resort investigate from storage Insight blade for the missing diagnostic settings and then enable.

## Key Vault Monitoring Deployment Agent

Key Vault diagnostic settings in Azure allow to configure monitoring for Azure Key Vault instances.

Like storage account diagnostic settings, this feature allows to collect various metrics and logs related to your Key Vault's usage, performance, and health.

Design Decision**:**

Diagnostics Settings enforcement will be achieved by following:

1. Enforcement of diagnostics settings (all Metric) via code during deployment
2. Optionally enforce by policy and user managed identity with condition of “If not exists”.
3. At a last resort investigate from storage Insight blade for the missing diagnostic settings and then enable.

# Azure Monitor Access Control

Azure Monitoring Access Control refers to the management of permissions and access rights related to Azure Monitor resources and functionalities.

This access control mechanism allows to define who can view, manage, and take actions on monitoring data, alerts, dashboards.

The built in monitoring roles are as below:

* Monitoring Reader
* Monitoring Contributor

Design Decision**:**

Azure Monitoring will mainly be used by IT Operations and Security Team. For that reason, its suggested to use a Security Group that has Monitoring Contributor RBAC role and assign users to this security groups that are responsible for Azure Monitoring.

# Azure Monitor Security Control

Azure Monitor Security Control intends to secure the security monitoring Logs so they cannot be accidently deleted or edited by users that has access to Azure Monitor.

Design Decision**:**

Azure Monitor Logs must be exported to a Storage Account. Access to the Storage Account should be controlled by the existing Access Review process.

# Architecture Acceptance

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

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

Implementation will begin once proposed architecture is accepted & document signed.

|  |  |
| --- | --- |
| **Project** | Governance Design |
| **Document Version** | 1.0 |

**Signed on behalf of ​Ambulance Victoria​**

|  |  |
| --- | --- |
| **Name** | Dan Howarth |
| **Position** |  |
| **Signature** | Microsoft Office Signature Line... |
| **Date signed** |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| **Name** | Jeff Chowdhury |
| **Position** | Infrastructure & Cloud Architect |
| **Signature** | Microsoft Office Signature Line... |
| **Date signed** |  |