**CORE SERVICE DESIGN:**

**Azure Update Manager**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Update Manager Core Service Design |
| **File Name** | Ambulance Victoria – Azure Update Manager Core Service Design v3.0.docx |
| **Version** | 3.0 |
| **Status** | Updated |
| **Release Date** | 21/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 8/02/2024 |
| 2.0 | Updated | Minor feedback | 17-20 | 14/02/2024 |
| 3.0 | Updated | Added existing patching groups | 18-27 | 21/02/2024 |

Table of Contents

[1. Overview 5](#_Toc159399619)

[1.1 Purpose and Audience 5](#_Toc159399620)

[1.2 Scope and Key Deliverables 5](#_Toc159399621)

[1.3 Glossary and Definitions 6](#_Toc159399622)

[2. Executive Summary 7](#_Toc159399623)

[3. Resource Cost 8](#_Toc159399624)

[4. WAF and Security Control Alignment 8](#_Toc159399625)

[4.1 Reliability 9](#_Toc159399626)

[4.1.1 Overview 9](#_Toc159399627)

[4.1.2 Azure Update Manager Reliability Checklist 9](#_Toc159399628)

[4.2 Cost Optimisation 9](#_Toc159399629)

[4.2.1 Overview 9](#_Toc159399630)

[4.2.2 Azure Update Manager Cost Optimisation Checklist 9](#_Toc159399631)

[4.3 Operational Excellence 10](#_Toc159399632)

[4.3.1 Overview 10](#_Toc159399633)

[4.3.2 Azure Update Manager Operational Excellence Checklist 10](#_Toc159399634)

[4.4 Performance Efficiency 10](#_Toc159399635)

[4.4.1 Overview 10](#_Toc159399636)

[4.4.2 Azure Update Manager Performance Efficiency Checklist 10](#_Toc159399637)

[4.5 Security 11](#_Toc159399638)

[4.5.1 Overview 11](#_Toc159399639)

[4.5.2 Azure Update Manager Security Checklist 11](#_Toc159399640)

[5. Architecture Summary 13](#_Toc159399641)

[5.1 Resource Overview 13](#_Toc159399642)

[5.2 RBAC 15](#_Toc159399643)

[5.3 Design Decisions and Justifications 15](#_Toc159399644)

[5.3.1 Periodic Assessment 15](#_Toc159399645)

[5.3.2 Exploits (Zero-Day) Patching 15](#_Toc159399646)

[5.3.3 Maintenance Configurations 16](#_Toc159399647)

[5.3.4 Customer Managed Schedules 16](#_Toc159399648)

[5.3.5 Dynamic Scoping 16](#_Toc159399649)

[6. Azure Policies 17](#_Toc159399650)

[7. Configuration Templates 18](#_Toc159399651)

[7.1 Windows Machine Schedules 18](#_Toc159399652)

[7.1.1 Maintenance Configuration - Prod - Full Automated A 18](#_Toc159399653)

[7.1.2 Maintenance Configuration - Prod - Full Automated B 19](#_Toc159399654)

[7.1.3 Maintenance Configuration - Prod - Full Automated C 20](#_Toc159399655)

[7.1.4 Maintenance Configuration -Test – Dev –Sandbox A 21](#_Toc159399656)

[7.1.5 Maintenance Configuration -Test – Dev –Sandbox B 22](#_Toc159399657)

[7.2 Linux Machine Schedules 23](#_Toc159399658)

[7.2.1 Maintenance Configuration - UP-DMZ AUTO 1 23](#_Toc159399659)

[7.2.2 Maintenance Configuration - UP-DMZ AUTO 2 24](#_Toc159399660)

[7.2.3 Maintenance Configuration - INFRA AUTO 1 25](#_Toc159399661)

[7.2.4 Maintenance Configuration - INFRA AUTO 2 26](#_Toc159399662)

[7.2.5 Maintenance Configuration - INFRA AUTO 3 27](#_Toc159399663)

[8. Acceptance 28](#_Toc159399664)

# Overview

This document covers the baseline design for the Azure Update Manager 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 Azure Update Manager 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 Azure Update Manager.

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 Azure Update Manager 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 Azure Update Manager 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 Security was relevant.

For this service the main baseline configurations include:

* Periodic assessment will be enabled on all machines, with an Azure Policy in place to auto-enrol any machines without this.
* Dynamic scoping will be used to add machines into their required patching schedule.

There are some notable differences across the service tier configurations for this service:

* Patching schedules will be different for Production and Non-Production. It is recommended that Non-Production is patched first to ensure that any issues with the patch are detected before Productions servers are patched.
* Tags will determine which schedule a given machine receives.

Note that there may be various scheduled required for different applications. The principles in this document can be used to create those maintenance configurations, as with the guidance in the Configuration Templates section.

# Resource Cost

The following details the pricing construct of servers covered by Azure Update Manager[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
| Service | Azure | Non-Azure |
| Azure Update Manager Server | Free | **$7.585**/server/month |
| **Per Server Fee** | Free if already purchased Microsoft Defender for Servers Plan 2  Or  $0.031/Server/hour Included data - 500 MB/day | Free if already purchased Microsoft Defender for Servers Plan 2  Or  $0.031/Server/hour Included data - 500 MB/day |

Table 2: Pricing construct

# 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

### Azure Update Manager Reliability Checklist

There is no Reliability guidance for Azure Update Manager under the Well-Architected Framework.

## 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

### Azure Update Manager Cost Optimisation Checklist

There is no Cost Optimisation guidance for Azure Update Manager under the Well-Architected Framework.

## 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

### Azure Update Manager Operational Excellence Checklist

There is no Operational Excellence guidance for Azure Update Manager under the Well-Architected Framework.

## 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

### Azure Update Manager Performance Efficiency Checklist

There is no Performance Efficiency guidance for Azure Update Manager under the Well-Architected Framework.

## 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.

### Azure Update Manager Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 4.1.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | Yes | No | Governance | Operational – as required |
| **S2** | 4.1.2 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. | Yes | Yes | IaC | At deployment |
| **S3** | 4.2.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. | Yes | Yes | IaC | At deployment |
| **S4** | 4.3.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists. | Yes | No | Governance | Operational – as reuqired |
| **S5** | 15.2.5 | Perform Automated Operating System & Application Patch Management | Yes | Yes | IaC | At deployment |

Table 3: Security checklist summary

# Architecture Summary

## Resource Overview

Azure Update Manager is the Azure service responsible for update monitoring and management[[7]](#footnote-8). It is capable of servicing Linux and Windows machines across both Azure and Non-Azure environments.

The following types of updates are supported:

* Operating System updates for Windows and Linux
* Extended Security Updates (ESU) for Windows Server
* First-party updates on Windows
* Third-party updates

The following shows the high-level flow of update management for a machine:

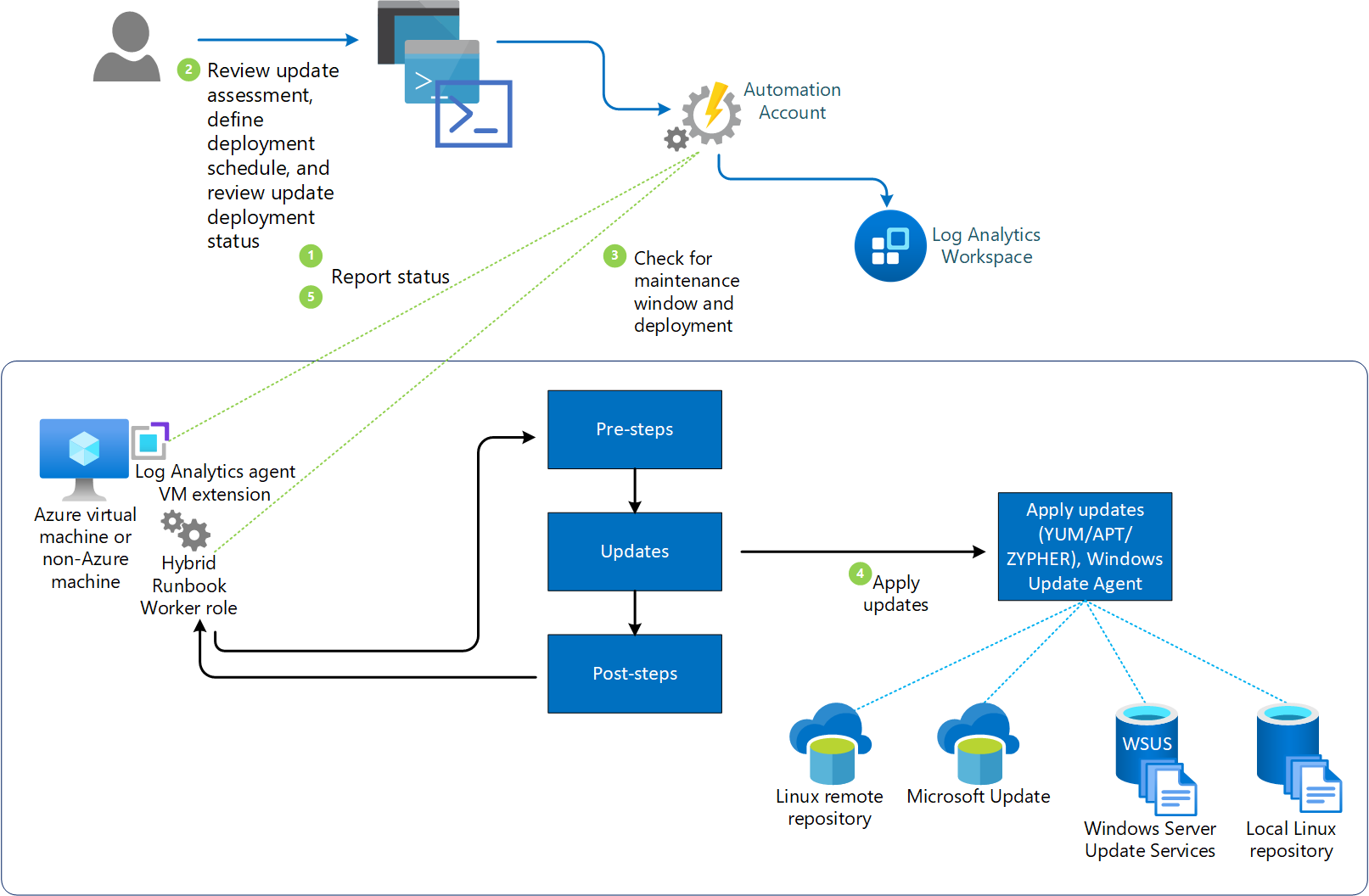


Figure 1: Automated updates flow summary

**Periodic Assessment[[8]](#footnote-9)**

Periodic Assessment allows Azure Update Manager to check for updates required on machines. It will fetch the latest updates every 24 hours and show the latest compliance status for each machine. Assessments or checks for updates can also be done manually and instantly if required more urgently.

**Update Options[[9]](#footnote-10)**

There are multiple options for updates that will depend on application-specific, as well as Operating System specific requirements.

***Automatic VM guest patching[[10]](#footnote-11)***

Enabling this for Azure VMs relaxes update management by atuatomically patching Vms to maintain security compliance. It has the following features:

* Critical or Security patches are automatically downloaded and applied on the VM.
* They are applied in off-peak hours for the time zone the VM is in.
* Any patch failures are automatically detected with health signals.
* This can be applied for a VM of any size.

This process happens every month as the new patches are released, and is completely automatic, including the reboot of the Virtual Machine. The patch will be installed within 30 days of the patch release, following an availability-first orchestration. The VM must be running during the off-peak hours for the patch to be installed. If there are no application-specific shut down requirements, this is the simplest patching method for IaaS VMs. This can be applied to a variety of Windows and Linux images.

***Automatic VM guest patching[[11]](#footnote-12)***

For Windows 2022 Datacenter Azure edition, another version of automatic patching known as Hotpatch can be applied.

**Dynamic Scoping**

Dynamic Scoping is a feature of Azure Update Manager that allows you to automatically pull Virtual Machines into a maintenance schedule with a pre-defined patching schedule based on Azure Tags.

## RBAC

There are no specific RBAC roles to be applied for this service. However, to onboard machines to this service, the following role or higher is required on the machine in question:

|  |  |
| --- | --- |
| Role | Scope |
| Azure Virtual Machine Contributor | Azure Virtual Machine |
| Azure Connected Machine Resource Administrator | Azure Arc-enabled server |

Table 4: RBAC roles applicable

## 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 Azure Update Manager 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.

### Periodic Assessment

**Design Reference:** Table 3 – [S5](#_Azure_Update_Manager)

**Design Decision:** Periodic Assessment will be configured for all patched machines.

**Design Justification:** Periodic Assessment ensures that machines are frequently checked for the latest patches available to them. The process happens every 24 hours to ensure that critical patches are not missed.

### Exploits (Zero-Day) Patching

**Design Reference:** Table 3 – [S1, S4](#_Azure_Update_Manager)

**Design Decision**: For zero-day exploits or specific vulnerabilities, there will need to be an internal process to patch these within 48 hours of a patch being released.

**Design Justification**: Azure Update Manager will be configured to perform periodic updates for standard patches. If there is an exploit and an immediate patch is required, this can be done manually using On-Demand patching within Azure Update Manager, however there will need to be an internal process to ensure that this is done for afflicted machines.

### Maintenance Configurations

**Design Reference:** Table 3 – [S5](#_Azure_Update_Manager)

**Design Decision:** Maintenance Configurations will be used to defined patching schedules and will be used with the Dynamic Scoping feature to automatically add machines into the required schedules.

**Design Justification:** Non-production workloads do not require Premium disks for operation.

**Design Details:** For standard patches that are released monthly, it is recommended to update Non-Production servers first to ensure that any issues present in the patch reveal themselves in a more easily fixable Non-Production server than in Production. Production servers should receive the patch the following week, so that they meet the requirement to be patched within 2 weeks of a new patch release.

### Customer Managed Schedules

**Design Reference:** Table 3 – [S5](#_Azure_Update_Manager)

**Design Decision:** Customer Managed Schedules will be used for customising automated patching cycles.

**Design Justification**: It can be risky to use completely automated Azure scheduled patching. Even Microsoft recommend for seamless experience that Customer Managed Schedules is the chosen value for patch orchestration. This is then used with Maintenance Configurations and Dynamic Scoping to automate the patching to the required internal schedules.

### Dynamic Scoping

**Design Reference:** Table 3 - [S5](#_Azure_Update_Manager)

**Design Decision:** Dynamic scoping will be used to add machines into Maintenance Configurations and patching cycles automatically.

**Design Justification:** It is a requirement to ensure that machines are patched automatically (where possible). To ensure that every machine onboarded into Azure Update Manager receives a maintenance configuration with an appropriate patching schedule, dynamic scoping will be used. The dynamic scoping will be based on machines that have a specific tag.

**Design Details:** There are two tags that will need to be used in conjunction to ensure that the correct Maintenance Configuration is applied via the Dynamic Scoping feature:

1. Automation\_Account: Value – the value of this will be the name of the automation account responsible for handling the automation.
2. Patching\_Group: Value – this will define which schedule the servers should follow.

# Azure Policies

The following Policies should be applied for this service:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Configure periodic checking for missing system updates on Azure virtual machines | av management group (under Root) |
| Schedule recurring updates using Azure Update Manager | av management group (under Root) |

Table 5: Azure Policies

# Configuration Templates

## Windows Machine Schedules

### Maintenance Configuration - Prod - Full Automated A

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-FullAutomatedA-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  Third  Tuesday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Windows  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: FullAutomatedA |

### Maintenance Configuration - Prod - Full Automated B

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-FullAutomatedB-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  Third  Wednesday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Windows  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: FullAutomatedB |

### Maintenance Configuration - Prod - Full Automated C

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-FullAutomatedC-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  Third  Thursday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Windows  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: FullAutomatedC |

### Maintenance Configuration -Test – Dev –Sandbox A

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-TestDevSandboxA-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  Second  Friday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Windows  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: TestDevSandboxA |

### Maintenance Configuration -Test – Dev –Sandbox B

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-TestDevSandboxB-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  Second  Saturday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Windows  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: TestDevSandboxB |

## Linux Machine Schedules

### Maintenance Configuration - UP-DMZ AUTO 1

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-UPDMZAUTO1-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Weekly  Monday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Linux  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: UPDMZAUTO1 |

### Maintenance Configuration - UP-DMZ AUTO 2

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-UPDMZAUTO2-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Weekly  Tuesday  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Linux  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: UPDMZAUTO2 |

### Maintenance Configuration - INFRA AUTO 1

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-INFRAAUTO01-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  1st  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Linux  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: INFRAAUTO01 |

### Maintenance Configuration - INFRA AUTO 2

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-INFRAAUTO02-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  8th  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Linux  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: INFRAAUTO02 |

### Maintenance Configuration - INFRA AUTO 3

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | mc-prd-ause-INFRAAUTO03-01 |
| **Subscription** | AV ALZ Management |
| **Resource Group** | rg-prd-ause-management-01 |
| **Region** | Australia Southeast |
| **Maintenance Scope** | Guest |
| **Reboot Setting** | Reboot if required |
| ***Schedule Settings*** |  |
| **Start Date** | ASAP |
| **Time Zone** | UTC+ 10:00 Canberra, Melbourne, Sydney |
| **Maintenance Window** | 3 hours 55 minutes |
| **Repeats** | Monthly  9th  No Offset  No end date |
| ***Dynamic Scope Settings*** |  |
| **Subscriptions** | Select all |
| **Filter By** | All resource groups  All resource types  Location: Australia Southeast  Linux  Selected tags:  Automation\_Account: aa-prd-ause-mgmt-01  Patching\_Group: INFRAAUTO03 |

# 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/azure-update-management-center/#:~:text=Azure%20Update%20Manager%20%28previously%20Azure%20Automation%3A%20Update%20Management%29,it%27s%20connected%20and%20managed%20by%20Azure%20Update%20Manager. [↑](#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/update-manager/overview?tabs=azure-vms [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/update-manager/assessment-options [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/virtual-machines/updates-maintenance-overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/windows-server/get-started/hotpatch?toc=%2Fazure%2Fvirtual-machines%2Ftoc.json [↑](#footnote-ref-12)