**CORE SERVICE DESIGN:**

**Recovery Services Vault and Backup**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Recovery Services Vault and Backup Core Service Design |
| **File Name** | Ambulance Victoria – Recovery Services Vault and Backup Core Service Design v1.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 7/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 2/02/2024 |
| 2.0 | Updated | Various feedback | 7, 17, 18, 20, 22-27 | 7/02/2024 |
| 2.1 | Final Update | Minor Feedback | 7, 21-27 | 7/02/2024 |

Table of Contents

[1. Overview 5](#_Toc158198602)

[1.1 Purpose and Audience 5](#_Toc158198603)

[1.2 Scope and Key Deliverables 5](#_Toc158198604)

[1.3 Glossary and Definitions 6](#_Toc158198605)

[2. Executive Summary 7](#_Toc158198606)

[3. Resource Cost 8](#_Toc158198607)

[4. WAF and Security Control Alignment 8](#_Toc158198608)

[4.1 Reliability 9](#_Toc158198609)

[4.1.1 Overview 9](#_Toc158198610)

[4.1.2 Recovery Services Vault and Backup Reliability Checklist 9](#_Toc158198611)

[4.2 Cost Optimisation 9](#_Toc158198612)

[4.2.1 Overview 9](#_Toc158198613)

[4.2.2 Recovery Services Vault and Backup Cost Optimisation Checklist 9](#_Toc158198614)

[4.3 Operational Excellence 10](#_Toc158198615)

[4.3.1 Overview 10](#_Toc158198616)

[4.3.2 Recovery Services Vault and Backup Operational Excellence Checklist 10](#_Toc158198617)

[4.4 Performance Efficiency 10](#_Toc158198618)

[4.4.1 Overview 10](#_Toc158198619)

[4.4.2 Recovery Services Vault and Backup Performance Efficiency Checklist 10](#_Toc158198620)

[4.5 Security 11](#_Toc158198621)

[4.5.1 Overview 11](#_Toc158198622)

[4.5.2 Recovery Services Vault and Backup Security Checklist 11](#_Toc158198623)

[5. Architecture Summary 14](#_Toc158198624)

[5.1 Resource Overview 14](#_Toc158198625)

[5.1.1 Recovery and Backup Vaults 14](#_Toc158198626)

[5.1.2 Azure Backup Service 14](#_Toc158198627)

[5.2 RBAC 15](#_Toc158198628)

[5.3 Design Decisions and Justifications 16](#_Toc158198629)

[5.3.1 Use of Vaults 16](#_Toc158198630)

[5.3.2 Backup Automation 16](#_Toc158198631)

[5.3.3 Disable public network access 17](#_Toc158198632)

[5.3.4 Managed Identity 17](#_Toc158198633)

[5.3.5 Immutability and Soft-Delete 18](#_Toc158198634)

[5.3.6 Redundancy 18](#_Toc158198635)

[5.3.7 Encryption 19](#_Toc158198636)

[5.3.8 Logging and Monitoring 19](#_Toc158198637)

[5.3.9 Azure Backup Access by RBAC 20](#_Toc158198638)

[5.3.10 Backup Policies 20](#_Toc158198639)

[6. Azure Policies 21](#_Toc158198640)

[7. Configuration Templates 22](#_Toc158198641)

[7.1 Primary Region Production Platinum RSV 22](#_Toc158198642)

[7.2 Secondary Region Production Platinum RSV 23](#_Toc158198643)

[7.3 Primary Region Production Gold/Silver RSV 24](#_Toc158198644)

[7.4 Primary Region Non-Production Bronze RSV 25](#_Toc158198645)

[7.5 Primary Region Production Platinum Backup Vault 26](#_Toc158198646)

[7.6 Secondary Region Production Platinum Backup Vault 26](#_Toc158198647)

[7.7 Secondary Region Production Gold/Silver Backup Vault 27](#_Toc158198648)

[7.8 Secondary Region Non-Production Bronze Backup Vault 27](#_Toc158198649)

[8. Acceptance 28](#_Toc158198650)

# Overview

This document covers the baseline design for the Recovery Services Vault and Backup 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 Recovery Services Vault and Backup 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 Recovery Services Vault and Backup.

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 Recovery Services Vault and Backup 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 |
| **RSV** | Recovery Services Vault |

Table : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Recovery Services Vault and Backup 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 Cost Optimisation and Security were relevant.

For this service the main baseline configurations include:

* Public access will be disabled.
* Vaults will be made to be permanently immutable.
* Backups will be automated per the Backup Policies.
* Soft delete will be enabled.

There are some notable differences across the service tiers and region deployments:

* Platinum, Gold, and Silver Primary Region vaults will be Geo-Redundant. Disaster Recovery region vaults will be Zone-Redundant. Bronze vaults will be Locally Redundant.
* Backup Policies for Azure Virtual Machines are aligned to the Public Records Office of Victoria guidelines.
* For Blob backups the retention periods will be set as follows:
  + Platinum – 360 days (maximum)
  + Gold/silver – 360 days (maximum)
  + Bronze – 30 days

For the Backup policies, there are already internal documents that should be referenced:

<https://intranet.ambulance.vic.gov.au/procedures/Procedures/PRO%20TAS%20004%20Data%20Backup.pdf>

# Resource Cost

The Vault’s themselves do not incur costs, but the Azure Backup service and the Storage of backups related to it do incur costs as shown in the following tables. It also depends on the Redundancy option chosen and whether that uses a Standard or Archive tier. The following prices are for Azure VM backups[[2]](#footnote-3):

|  |  |
| --- | --- |
| Size of each instance | Azure Backup price per month |
| Instance < or = 50 GB | **$7.2999** + storage consumed |
| Instance is > 50 GB but < or = 500 GB | **$14.5997** + storage consumed |
| Instance is > 500 GB | **$14.5997** for each 500 GB increment + storage consumed |

Table : Pricing construct per backup

|  |  |  |
| --- | --- | --- |
| Redundancy Option | Standard Tier | Archive Tier |
| LRS | **$0.0360** per GB | **$0.0057** per GB |
| ZRS | N/A per GB | N/A |
| GRS | **$0.0720** per GB | **$0.0097** per GB |
| RA-GRS | **$0.0914** per GB | **$0.0097** per GB |

Table : Pricing construct for storage tiers

# 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

### Recovery Services Vault and Backup Reliability Checklist

There is no specific Reliability guidance for Azure Backup or Recovery Services vaults. These services are inherently reliable.

## 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

### Recovery Services Vault and Backup Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Optimise costs with Reserved Instances | Yes | No | Governance | Operational – review monthly |

Table : 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.

### Recovery Services Vault and Backup Operational Excellence Checklist

There is no specific guidance for Operational Excellence for the Backup and Recovery services.

## Performance Efficiency

### Overview

Design for horizontal scaling 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:

* Run stress and performance tests.
* Continuously monitor performances, particularly in Production systems

### Recovery Services Vault and Backup Performance Efficiency Checklist

There is no specific guidance for Performance Efficiency for Azure Backup and Recovery Services Vaults.

## 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.

The following Microsoft Security Benchmark Controls are relevant:

* NS-2 Secure cloud services with network controls.
* IM-3 Manage application identities securely and automatically.
* DP-2 Monitor anomalies and threats targeting sensitive data.
* BR-1 Ensure regular automated backups.
* BR-2 Protect backup and recovery data.
* BR-3 Monitor backups.
* BR-4 Regularly test backup.

### Recovery Services Vault and Backup Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 5.1.1 | Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. | Yes | Yes | IaC | At deployment |
| **S2** | 5.1.2 | Restoration of important data, software, and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | No | Governance | Operational – every 6 months |
| **S3** | 5.1.3 | Unprivileged accounts cannot access backups belonging to other accounts. | Yes | No | Governance, IaC | Individual vaults deployed per application with RBAC assignments |
| **S4** | 5.1.4 | Unprivileged accounts are prevented from modifying and deleting backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S5** | 5.2.1 | Unprivileged accounts, and privileged accounts (excluding backup administrators), can only access their own backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S6** | 5.2.2 | Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S7** | 5.3.1 | Unprivileged accounts, and privileged accounts (excluding backup administrators), can’t access backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S8** | 5.3.2 | Unprivileged accounts, and privileged accounts (excluding backup break glass accounts), are prevented from modifying or deleting backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S10** | 19.1.1 | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational – every 6 months |
| **S11** | 16.3.4 | Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets. | Yes | No | Governance | Operational – quarterly |
| **S12** | 19.2.2 | Maintain a physically separate recovery site that enables ready restoration of key systems in the event that their availability is lost. | Yes | Yes | IaC | At deployment |
| **S13** | 19.3.1 | Maintain sufficient isolation of its recovery service / media, such that a cyber incident on its main network couldn’t impact the recovery service / media. | Yes | Yes | IaC | At deployment |
| **S14** | 19.3.2 | Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services. | Yes | Yes | IaC | At deployment |

Table : Security checklist summary

# Architecture Summary

## Resource Overview

### Recovery and Backup Vaults

Note that there are two types of Vaults in Azure:

* Azure Recovery Services Vault
* Azure Backup Vault

They are both used for backup and recovery in Azure but there are some slight differences. The difference is in the data sources that are available in each vault and the use-cases[[7]](#footnote-8).

Azure Recovery Services Vaults can be used for Azure Backup and Site Recovery data. Azure Backup Vaults are for Azure Backup data only[[8]](#footnote-9).

The following table shows what data each type of Vault is able to support:

|  |  |
| --- | --- |
| Recovery Services vault | Backup vault |
| Azure Virtual Machine | Azure Disks |
| SQL in Azure VM | Azure Blobs |
| Azure Files | Azure Database for PostgreSQL server |
| SAP HANA in Azure VM | Kubernetes services |
| Azure Backup server |  |
| Azure Backup agent |  |
| Data Protection Manager (DPM) |  |

Table : Comparison of data available in Vaults

### Azure Backup Service

Azure Backup is a separate service to the Vaults previously mentioned. It is the service that facilitates backup data being stored in Vaults[[9]](#footnote-10). It is possible to backup the following services using Azure Backup:

* On-premises – files, folders, system state. Requires an agent to be installed.
* Azure VMs – Linux and Windows
* Azure Managed Disks
* Azure Files shares
* SQL Server in Azure VMs
* SAP HANA databases in Azure VMs
* Azure Database for PostgreSQL servers
* Azure Blobs
* Azure Database for PostgreSQL Flexible server
* Azure Kubernetes service

Azure Backup uses Azure Storage to host the backup instances, and has multiple replication options as with any regular Azure Storage account:

* LRS
* ZRS
* GRS/RAGRS

## RBAC

Azure Backup has three built-in roles to control backup management operations[[10]](#footnote-11):

|  |  |  |
| --- | --- | --- |
| Role Name | Description | Scope |
| Backup Contributor | This role has all permissions to create and manage backup except deleting Recovery Services vault and giving access to others. Imagine this role as admin of backup management who can do every backup management operation. | Recovery Services Vault  Backup Vault |
| Backup Operator | This role has permissions to everything a contributor does except removing backup and managing backup policies. This role is equivalent to contributor except it can't perform destructive operations such as stop backup with delete data or remove registration of on-premises resources. | Recovery Services Vault  Backup Vault |
| Backup Reader | This role has permissions to view all backup management operations. Imagine this role to be a monitoring person. | Recovery Services Vault  Backup Vault |
| Disk Backup Reader | Provides permission to back up vault to perform disk backup. | Azure Disks |
| Disk Pool Operator | Provide permission to StoragePool Resource Provider to manage disks added to a disk pool. | Azure Disks |
| Disk Restore Operator | Provides permission to back up vault to perform disk restore. | Azure Disks |
| Disk Snapshot Contributor | Provides permission to back up vault to manage disk snapshots. | Azure Disk Snapshots |
| Storage Account Backup Contributor | Lets you perform backup and restore operations using Azure Backup on the storage account. | Storage Accounts |

Table : 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 Recovery Services Vault and Backup 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.

### Use of Vaults

**Design Reference:** N/A

**Design Decision**: Both types of Backup Vaults will be used.

**Design Justification**: The Recovery Services Vault and the Backup Vault will both need to be used to back up the required resources. RSVs will be used for VM Backups primarily, and the Backup Vaults will be used for other resources that require backup such as the Blob services.

### Backup Automation

**Design Reference:** Microsoft Security Benchmark BR-1

**Design Decision:** Backup will be configured to automatically backup the relevant resources. Additionally, an automation via Azure Policy can be put in place to automatically enrol resources such as Azure Virtual Machines, into Azure Backup upon creation.

**Design Justification:** Automated backups reduce the risk of missed backups compared to manually backing up servers and other resources daily or at different time intervals. Using Azure Policy to control which VMs are enrolled in backup also decreases the chance that a Virtual Machine will be missed. The Policy can be set to make VMs receive a backup policy from a RSV in the same location (Subscription and Region). This can be done either by forcing VMs with a tag, or forcing VMs without a tag, to enrol in backup, depending on preference[[11]](#footnote-12).

**Design Details:** To ensure that no machines are missed, there will be two policies in place.

Policy 1: *Configure backup on VMs with a given tag to an existing recovery services vault in the same location*

This Policy will ensure that machines with a specific tag will be enrolled in their specified backup policy. There will be three versions of this tag:

Backup\_Policy: Platinum

Backup\_Policy: Gold/Silver

Backup\_Policy: Bronze

The value of the tag will determine which backup policy is applied.

Policy 2: *Configure backup on VMs without a given tag to an existing recovery services vault in the same location*

This policy will act as a failsafe. This is in case a machine is not given a tag so the first policy will not enrol them in a recovery vault. This will default enrol machines into the Platinum policy as the most secure one.

### Disable public network access

**Design Reference:** Microsoft Security Benchmark [NS-2](#_Recovery_Services_Vault)

**Design Decision:** Public Network access will be denied. Private Endpoints will be used in the spoke closest to the resource being used, as defined in the Private Endpoint Core Service design. This will require a Managed Identity to facilitate access.

**Design Justification:** Public access to sensitive recovery data is against security best practices and unnecessarily leaves the environment open to malicious access. As such, public access will be denied. Private Endpoints will be used for access to Recovery Services vaults as this is the most secure method of access. They will be placed closest to the resource being used as is the standard architecture for Ambulance Victoria. Note that the use of Private Endpoints may have impacts to network design.

### Managed Identity

**Design Reference:** Microsoft Security Benchmark IM-3

**Design Decision:** Managed Identities will be enabled for Vaults.

**Design Justification:** Allowing managed identities will allow the vault to create and use private endpoints as the most secure method of access, as discussed in a previous design decision[[12]](#footnote-13). The Managed Identity must also be granted Contributor permissions on the vault. This is more secure than using a service principle as Microsoft manage and rotate the secrets of the Managed Identity and removes the requirement for the customer to manage secrets and keys of Service Principals.

### Immutability and Soft-Delete

**Design Reference:** Microsoft Security Benchmark [DP-2](#_Recovery_Services_Vault), Table 6 - [S4, S6, S8, S14](#_Recovery_Services_Vault)

**Design Decision:** Recovery Vaults will be made to be permanently immutable and will have the soft-delete function enabled.

**Design Justification:** Making a vault immutable prevents users from modifying or removing any previous backup points. The immutability can be a reversible operation, but it is recommended here to make it irreversible so that potentially malicious actors will not be able to make any changes by disabling immutability settings.

Additionally, soft-delete will be enabled to ensure that there is no accidental deletion of a vault, and that it can be recovered within the soft-delete period thus preventing unnecessary data loss.

**Design Details:** For soft delete the following will be applied depending on the service catalog tier:

* Platinum – 30 days
* Gold/Silver – 14 days
* Bronze – 7 days

Note that for permanent immutability, this will only be applied to Platinum, Gold, and Silver, or any Production service. It is not required for Non-Production.

Additionally, a resource lock can be implemented to ensure there is no accidental deletion.

### Redundancy

**Design Reference:** Table 6 - S12

**Design Decision:** The Vaults created in Australia Southeast for Platinum, Gold, or Silver operations will be set as Geo-Redundant. Bronze services will be set as Locally-Redundant. For the Australia East region, for critical workloads, Zone-Redundant can be used, and Locally-Redundant for less critical workloads.

**Design Justification:** Australia Southeast does not currently have capability to perform Zone-Redundancy. As such, for Production workloads it should be set to Geo-Redundant. This not only provides coverage in case of a regional outage, it also meets the Department of Health controls requiring that there is a physically separate location in which backup data is stored.

### Encryption

**Design Reference:** Microsoft Security Benchmark [DP-3, DP-4](#_Recovery_Services_Vault)

**Design Decision:** Data is encrypted by default in Azure Backup[[13]](#footnote-14).

**Design Justification:** Data is encrypted inherently on two levels within Azure Backup. Encryption of Data in the Recovery Services Vault, and Encryption specific to the workload being backed-up. As such no additional configurations are required to meet these controls.

Transfer of data between the Vault and the Azure Storage is also protected by HTTPS and never leaves the Azure network, so no additional configurations are required for data in transit for this service either[[14]](#footnote-15).

### Logging and Monitoring

**Design Reference:** Microsoft Security Benchmark LT-4

**Design Decision:** Monitoring is built into Azure Backup functions. Diagnostic settings will be created for RSV and Backup Vaults. Additionally, an alert will be configured for backup data being deleted, and another for backup failures.

**Design Justification:** There are several monitoring operations that are pre-deployed and native to Azure. Azure Advisor will also provide hourly recommendations on VMs that aren’t backed up without requiring any specific configuration. The recommendations can also be dismissed for a period and will return later after a specified timeframe.

Diagnostics will be enabled for Recovery Services Vaults and forwarded to the central Log Analytics Workspace for that region.

Additionally, the Backup Jobs pane in Backup Centre allows you to view recent backup and restore operations and their statuses in the Azure Portal.

For monitoring the main two alerts that will be configured are to alert when backup data has been purged or deleted, and for when backup jobs fail.

### Azure Backup Access by RBAC

**Design Reference:** Table 6 – [S3-S8](#_Recovery_Services_Vault)

**Design Decision:** RBAC will be used to granularly control which users can perform which kinds of backup operations.

**Design Justification:** The roles listed in Section 5.2 define the scope at which certain roles can perform backups. Some will only be able to perform backup on Azure Disks, some on Azure Storage, or some on any service that can be backed up, depending on internal requirements. This meets the Department of Health controls which prevents users from being able to modify other backups. This in addition to the Immutability setting will prevent accidental or malicious modification of backup points.

### Backup Policies

**Design Reference:** N/A

**Design Decision:** Policies for Virtual Machines and Blobs will be defined here. Others will be defined as specific services are required.

**Design Justification:** Backup Policies are required to be implemented for the VMs and other resources to be automatically backed up at the desired frequency and retentions.

**Design Details:**

**Virtual Machine Backups**

For Azure VMs the following Policies are recommended standards. Note that Ambulance Victoria may have different requirements per application, and additional policies may be added to the standard set deployed for each vault as approved.

**Platinum (bkpol-platinum-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 31 days |
| Weekly | Sunday at 1:00am AEST | 5 weeks |
| Monthly | First Sunday at 1:00am AEST | 6 months |
| Yearly | Last Sunday of January and Last Sunday of July at 1:00am AEST | 6 months |

**Gold/Silver (bkpol-goldsilver-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 14 days |
| Weekly | Sunday at 1:00am AEST | 4 weeks |
| Monthly | First Sunday at 1:00am AEST | 6 months |
| Yearly | Last Sunday of January and Last Sunday of July at 1:00am AEST | 6 months |

**Bronze (bkpol-bronze-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 7 days |
| Weekly | Sunday at 1:00am AEST | 4 weeks |
| Monthly |  | 0 months |
| Yearly |  | 0 years |

**Blob Backups**

For Blob backups, as mentioned in the Storage and Blob Core Service design document, the backups will be set as Operational backups which do not require a schedule. The default retention is 30 days, but the following values will be used for the different tiers:

* Platinum – 360 days (bkpol-platinum-blob)
* Gold/silver – 360 days (bkpol-goldsilver-blob)
* Bronze – 30 days (bkpol-bronze-blob)

# Azure Policies

There following built-in policies should be leveraged to automate backups being enabled on VMs:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Configure backup on VMs with a given tag to an existing recovery services vault in the same location | av management group (under Root) |
| Configure backup on VMs without a given tag to an existing recovery services vault in the same location | av management group (under Root) |

Table : Azure Policies

# Configuration Templates

## Primary Region Production Platinum RSV

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | rsv-prd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Geo-redundant |
| Cross-Region Restore | Enabled |
| Enable Immutability | Enabled |
| Encryption Type | Microsoft Managed Key |
| **PRIVATE CONNECTIVITY** |  |
| Connectivity Method | Deny public access and allow private access |
| Private endpoint | pep-prd-ause-[appname]-rsv-01 |
| Target Sub-resource | AzureBackup |
| Virtual Network | vnet-prd-ause-[appname]-01 |
| Subnet | snet-prd-ause-[appname]-[workload]-01 |
| Private DNS Zones | privatelink.ase.backup.windowsazure.com  privatelink.queue.core.windows.net  privatelink.blob.core.windows.net |
| Private DNS Zone Subscription | AV ALZ Connectivity |
| Private DNS Zone Resource Group | rg-prd-ause-connectivity-privatedns-01 |

**Backup Policy – Platinum (bkpol-platinum-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 31 days |
| Weekly | Sunday at 1:00am AEST | 5 weeks |
| Monthly | First Sunday at 1:00am AEST | 6 months |
| Yearly | Last Sunday of January and Last Sunday of July at 1:00am AEST | 6 months |

## Secondary Region Production Platinum RSV

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | rsv-dr-auea-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-auea-infra-rsv-01 |
| Backup Storage Redundancy | Zone-Redundant |
| Cross-Region Restore | Disabled |
| Enable Immutability | Enabled |
| Encryption Type | Microsoft Managed Key |
| **PRIVATE CONNECTIVITY** |  |
| Connectivity Method | Deny public access and allow private access |
| Private endpoint | pep-dr-auea-[appname]-rsv-01 |
| Target Sub-resource | AzureBackup |
| Virtual Network | vnet-dr-auea-[appname]-01 |
| Subnet | snet-dr-auea-[appname]-[workload]-01 |
| Private DNS Zones | privatelink.ase.backup.windowsazure.com  privatelink.queue.core.windows.net  privatelink.blob.core.windows.net |
| Private DNS Zone Subscription | AV ALZ Connectivity |
| Private DNS Zone Resource Group | rg-prd-auea-connectivity-privatedns-01 |

**Backup Policy – Platinum (bkpol-platinum-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 31 days |
| Weekly | Sunday at 1:00am AEST | 5 weeks |
| Monthly | First Sunday at 1:00am AEST | 6 months |
| Yearly | Last Sunday of January and Last Sunday of July at 1:00am AEST | 6 months |

## Primary Region Production Gold/Silver RSV

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | rsv-prd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Geo-redundant |
| Cross-Region Restore | Disabled |
| Enable Immutability | Enabled |
| Encryption Type | Microsoft Managed Key |
| **PRIVATE CONNECTIVITY** |  |
| Connectivity Method | Deny public access and allow private access |
| Private endpoint | pep-prd-ause-[appname]-rsv-01 |
| Target Sub-resource | AzureBackup |
| Virtual Network | vnet-prd-ause-[appname]-01 |
| Subnet | snet-prd-ause-[appname]-[workload]-01 |
| Private DNS Zones | privatelink.ase.backup.windowsazure.com  privatelink.queue.core.windows.net  privatelink.blob.core.windows.net |
| Private DNS Zone Subscription | AV ALZ Connectivity |
| Private DNS Zone Resource Group | rg-prd-ause-connectivity-privatedns-01 |

**Gold/Silver (bkpol-goldsilver-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 14 days |
| Weekly | Sunday at 1:00am AEST | 4 weeks |
| Monthly | First Sunday at 1:00am AEST | 6 months |
| Yearly | Last Sunday of January and Last Sunday of July at 1:00am AEST | 6 months |

## Primary Region Non-Production Bronze RSV

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | rsv-npd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-npd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Locally Redundant |
| Cross-Region Restore | Disabled |
| Enable Immutability | Disabled |
| Encryption Type | Microsoft Managed Key |
| **PRIVATE CONNECTIVITY** |  |
| Connectivity Method | Deny public access and allow private access |
| Private endpoint | pep-npd-ause-[appname]-rsv-01 |
| Target Sub-resource | AzureBackup |
| Virtual Network | vnet-npd-ause-[appname]-01 |
| Subnet | snet-npd-ause-[appname]-[workload]-01 |
| Private DNS Zones | privatelink.ase.backup.windowsazure.com  privatelink.queue.core.windows.net  privatelink.blob.core.windows.net |
| Private DNS Zone Subscription | AV ALZ Connectivity |
| Private DNS Zone Resource Group | rg-prd-ause-connectivity-privatedns-01 |

**Bronze (bkpol-bronze-VM)**

|  |  |  |
| --- | --- | --- |
| Frequency | Occurs | Retain For |
| Daily | 1:00am AEST | 7 days |
| Weekly | Sunday at 1:00am AEST | 4 weeks |
| Monthly |  | 0 months |
| Yearly |  | 0 years |

## Primary Region Production Platinum Backup Vault

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | bvault-prd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Geo-redundant |
| Soft delete | Enabled – 30 days |
| Enable Immutability | Enabled |
| Managed Identity | Enabled – System Assigned |
| Encryption | Microsoft Managed Key |
| Cross Region Restore | Enabled |
| **Blob Backup Policy Details** |  |
| Name | bkpol-platinum-blob |
| Type | Operational |
| Retention | 30 days |

## Secondary Region Production Platinum Backup Vault

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | bvault-prd-auea-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-auea-infra-rsv-01 |
| Backup Storage Redundancy | Zone-redundant |
| Soft delete | Enabled – 30 days |
| Enable Immutability | Enabled |
| Managed Identity | Enabled – System Assigned |
| Encryption | Microsoft Managed Key |
| Cross Region Restore | Enabled |
| **Blob Backup Policy Details** |  |
| Name | bkpol-platinum-blob |
| Type | Operational |
| Retention | 360 days |

## Secondary Region Production Gold/Silver Backup Vault

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | bvault-prd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-prd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Geo-redundant |
| Soft delete | Enabled – 14 days |
| Enable Immutability | Enabled |
| Managed Identity | Enabled – System Assigned |
| Encryption | Microsoft Managed Key |
| Cross Region Restore | Enabled |
| **Blob Backup Policy Details** |  |
| Name | bkpol-goldsilver-blob |
| Type | Operational |
| Retention | 360 days |

## Secondary Region Non-Production Bronze Backup Vault

|  |  |
| --- | --- |
| Configuration item | Configuration Setting |
| Name | bvault-npd-ause-infra-01 |
| Subscription | AV ALZ [Subscription Name] |
| Resource Group | rg-npd-ause-infra-rsv-01 |
| Backup Storage Redundancy | Locally-redundant |
| Soft delete | Enabled – 7 days |
| Enable Immutability | Disabled |
| Managed Identity | Enabled – System Assigned |
| Encryption | Microsoft Managed Key |
| Cross Region Restore | Enabled |
| **Blob Backup Policy Details** |  |
| Name | bkpol-bronze-blob |
| Type | Operational |
| Retention | 7 days |

# 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 | 2.0 |

**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/backup/ [↑](#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/answers/questions/405915/what-is-difference-between-recovery-services-vault [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/reliability/reliability-backup?toc=%2Fazure%2Fbackup%2Ftoc.json&bc=%2Fazure%2Fbackup%2Fbreadcrumb%2Ftoc.json [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/backup/backup-overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/backup/backup-azure-auto-enable-backup [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/azure/backup/private-endpoints [↑](#footnote-ref-13)
13. https://learn.microsoft.com/en-us/azure/backup/backup-encryption [↑](#footnote-ref-14)
14. https://learn.microsoft.com/en-us/azure/backup/guidance-best-practices [↑](#footnote-ref-15)