**Azure Site Recovery High Level Design**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Site Recovery High Level Design |
| **File Name** | Ambulance Victoria – Azure Site Recovery High Level Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Draft |
| **Release Date** | 06/05/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 06/05/2024 |

Table of Contents

[1. Overview 4](#_Toc166056644)

[1.1 Purpose and Audience 4](#_Toc166056645)

[1.2 Scope and Key Deliverables 4](#_Toc166056646)

[1.3 Glossary and Definitions 5](#_Toc166056647)

[2. Executive Summary 6](#_Toc166056648)

[2.1 Disaster Recovery 6](#_Toc166056649)

[3. Resource Cost 7](#_Toc166056650)

[4. Architecture Summary 7](#_Toc166056651)

[4.1 Resource Overview 7](#_Toc166056652)

[4.2 Solution Diagram 8](#_Toc166056653)

[4.3 RBAC 9](#_Toc166056654)

[4.4 Design Decisions and Justifications 10](#_Toc166056655)

[5. Azure Policies 11](#_Toc166056656)

[6. Configuration Templates 12](#_Toc166056657)

[6.1 Azure Policy Settings 12](#_Toc166056658)

[6.2 Platinum Retention Policy Settings 13](#_Toc166056659)

[6.3 Gold/Silver Retention Policy Settings 13](#_Toc166056660)

[6.4 RTO and RPO matrix 14](#_Toc166056661)

[7. Acceptance 14](#_Toc166056662)

# Overview

This document covers the baseline design for the Azure Site Recovery High Level Design 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 Site Recovery High Level Design 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 Site Recovery High Level Design.

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 high level deployment requirements and the details for the Azure Site Recovery High Level Design 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 |
| **DR** | Disaster Recovery |
| **DRP** | Disaster Recovery Plan |
| **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 |
| **ASR** | Azure Site Recovery |
| **RTO** | Recovery Time Objective |
| **RPO** | Recovery Point Objective |

Table 1: Glossary and definitions

# Executive Summary

This design outlines the baseline standards for the Azure Site Recovery (ASR) High-Level Design Core Service, following an assessment against the five pillars of the Well-Architected Framework (WAF) and the Department of Health Security Controls. The key design decisions are summarized below:

**1. ASR for Production Workloads:** ASR will be utilized for Production workloads to ensure business continuity and disaster recovery readiness.

**2. Alternative Recovery Options:** While ASR is recommended for Production workloads, other services, including Platinum services, can also be recovered using Azure Backup, providing flexibility in recovery options.

**3. Workload Assessment:** Each workload should be individually assessed to determine if ASR is required based on its Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

**4. RTO and RPO Testing:** ASR configurations should be tested against pre-defined RTO and RPO targets to ensure they meet the desired recovery objectives.

**5. Non-Production Workloads:** ASR should not be configured for Non-Production or Bronze workloads, limiting its use to critical production environments.

**6. Deployment Methods:** ASR cannot be deployed using Bicep and must be configured via the Azure policy or for remediation it can also be done manually through the portal, PowerShell. However, caution should be exercised when using Azure Policy to avoid enforcing ASR on all new Virtual Machines unless it meets a specific requirement.

## Disaster Recovery

Note that ASR on its own does **NOT** meet Disaster Recovery requirements, only the infrastructure failover for Virtual Machines. An overall Disaster Recovery and Business Continuity agenda needs to be created considering not only how to recover each application, but also the order in which applications need to be brought back ordered by priority.

Each application should have its own individual runbook as well as regular failover testing to ensure that it can be recovered in case of component failover, as well as in the case of a full regional outage.

Some components to be considered for an overall Disaster Recovery runbook and planning are:

* ASR and backup enablement of infrastructure
* Application layer requirements and sequencing
* RTO and RPO definitions
* Failover test planning
* Communications plans
* Application recovery prioritisation
* Updated DRP for each application landing zone design
* Recovery type for each application: active-active, active-passive etc.
* Whether the application needs recovery or if it has innate availability

**Additional References:**

* [Pages - Guides, Tools and Templates (ambulance.vic.gov.au)](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fsites%2FTeams%2Fem%2Fbr%2FPages%2FGuides--Tools.aspx&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107345699%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=AJUAGRqZA%2Br0p%2FSarndK88dtAxWbl747s26IYMt3Oyw%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/PRO%20TAS%20004%20Data%20Backup.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FPRO%2520TAS%2520004%2520Data%2520Backup.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107360478%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=iZKnqBfZ1wXJyBkd8Gi%2BysaNCmyiBK6JPm%2BpdfgvWrM%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/FRA%20DTS%20001%20DTS%20Business%20Service%20Catalogue.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FFRA%2520DTS%2520001%2520DTS%2520Business%2520Service%2520Catalogue.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107371428%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=GbKUL0hLiCRNiYQOamwgAT9umCJGNYL2q%2BxWxYT4eRk%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/POL%20FCS%20079%20Business%20Resilience%20Policy.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FPOL%2520FCS%2520079%2520Business%2520Resilience%2520Policy.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107382868%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Wc%2ByO8ZzDf06msbHs6j3Jejc5pAkcp8ENvLyCUsAGQA%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/sites/Teams/IT/ICT%20Documentation/Cybersecurity%20Policies%20and%20Standards%20Implementation/POL%20DTS%20001%20Backup%20and%20Recovery%20Policy.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fsites%2FTeams%2FIT%2FICT%2520Documentation%2FCybersecurity%2520Policies%2520and%2520Standards%2520Implementation%2FPOL%2520DTS%2520001%2520Backup%2520and%2520Recovery%2520Policy.pdf%23search%3DPOL%252FDTS&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107393493%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Cudk%2BX6Fak%2BxNyvhKD6P2Z7imEafzNgTNAY7%2BdK8ldU%3D&reserved=0)

# Resource Cost

The following table shows the pricing construct for Azure Site Recovery[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
|  | Price For First 31 days | Price After 31 Days |
| Azure Site Recovery to customer owned sites | Free | **$23.360**/month per instance protected |
| Azure Site Recovery to Azure | Free | **$36.500**/month per instance protected |

Table 2: Pricing Construct

As we will be using Azure site recovery to Azure, the below cost applies.

**$36.500**/month per instance protected

# Architecture Summary

## Resource Overview

Azure Site Recovery (ASR) is an Azure-native service that supports Business Continuity and Disaster Recovery (BCDR) strategies for both planned and unplanned outages. It enables us to manage replication, failover, and failback for services that have this capability enabled. ASR can be used for Azure Virtual Machines (VMs) as well as for On-Premises replication. It also allows us to test Disaster Recovery and run drills without impacting the live replication of machines.

Key Features:

* Replication Management: ASR facilitates the management of replication settings for VMs, ensuring data is continuously replicated to a recovery site.
* Failover and Failback: ASR enables failover and failback processes, ensuring minimal downtime during disaster recovery scenarios.
* Testing and Drills: ASR supports testing and running drills for Disaster Recovery without affecting the live environment, ensuring readiness for real-world scenarios.
* Customized Failover: ASR allows for customized failover plans, ensuring that the sequence of multi-tiered applications is failed over correctly, maintaining application consistency.

## Solution Diagram

Figure 1: ASR from Primary Region to Secondary Region

## RBAC

For Azure Site Recovery the following roles are applicable[[3]](#footnote-4):

|  |  |
| --- | --- |
| Role Name | Description |
| Site Recovery Contributor | Lets you manage Site Recovery service except vault creation and role assignment. |
| Site Recovery Operator | Lets you failover and failback but not perform other Site Recovery management operations. |
| Site Recovery Reader | Lets you view Site Recovery status but not perform other management operations. |

* Role Assignments:- Below role need to be assigned to the respective teams.

Infra cloud team -- Site Recovery Contributor, Site Recovery Contributor

Security team --- Site Recovery Reader.

To assign the roles to the respective teams, follow these steps:

1. **Assign Site Recovery Contributor Role to Infra Cloud Team:**
   * Go to the Azure portal and navigate to the subscription or resource group where Azure Site Recovery is configured.
   * Click on "Access control (IAM)" in the left-hand menu.
   * Click on the "Add" button, then select "Add role assignment".
   * In the "Role" dropdown, select "Site Recovery Contributor".
   * In the "Assign access to" dropdown, select the appropriate scope (subscription or resource group).
   * In the "Select" dropdown, search for and select the Infra Cloud Team's Azure AD group or user account.
   * Click "Save" to assign the role.
2. **Assign Site Recovery Reader Role to Security Team:**
   * Follow the same steps as above but select "Site Recovery Reader" as the role instead.
   * Assign this role to the Security team's Azure AD group or user account.

## Design Decisions and Justifications

1. **Azure Site Recovery Regions:**

Design Decision: Australia East is designated as the Disaster Recovery region.

Justification: Australia Southeast is the primary region for Ambulance Victoria. ASR is configured to failover to Australia East for disaster recovery, meeting the security control of having two physically separate recovery regions.

2**. ASR Churn:**

Design Decision: Churn support will not be enabled by default and will only be enabled for workloads that require it.

Justification: Churn, the data change rate, is default supported at 54 MB/s per VM. High Churn (up to 100 MB/s) can be manually enabled in the portal for workloads requiring it.

3. **Azure Site Recovery Use:**

Design Decision: ASR should be used for applications with specific RTO and RPO requirements, primarily for Production workloads.

Justification: ASR should not be configured for every workload by default. It should be assessed and tested against RTO and RPO. Enable for Platinum workloads; consider Gold and Silver workloads case-by-case; not recommended for Non-Production workloads.

4. **Deploying Azure Site Recovery:**

Design Decision: ASR should be used for applications with specific RTO and RPO requirements, likely Platinum workloads.

Justification: Bicep does not directly support deploying ASR. Use PowerShell or Azure Policy. Azure Policy is recommended with a built-in policy applied at the root management group to specify only machines with a specific tag have ASR enabled.

5. **Change Management:**

Any changes, modifications, or removals from the pre-approved deployments require specific approval from the Cloud Governance Forum before deployment.

These design decisions and justifications form the baseline requirements for Azure Site Recovery in alignment with WAF and Security controls. They ensure that ASR is deployed appropriately for applications with specific RTO and RPO requirements, enabling efficient disaster recovery and maintaining operational excellence.

# Azure Policies

The following built-in Azure Policy must be used if it is preferable to using PowerShell during deployments:

|  |  |
| --- | --- |
| Policy Name | Description |
| Configure disaster recovery on virtual machines by enabling replication via Azure Site Recovery | Virtual machines without disaster recovery configurations are vulnerable to outages and other disruptions. If the virtual machine does not already have disaster recovery configured, this would initiate the same by enabling replication using preset configurations to facilitate business continuity. You can optionally include/exclude virtual machines containing a specified tag to control the scope of assignment. |

For this Policy it is recommended to apply to Production Virtual Machines. The settings within this policy can be configured so that only machines with a specific tag will have this enabled. As discussed in this document, ASR is not recommended to be the default enablement across all servers, only specific servers that have this as a requirement.

1. **Policy Name**: Configure disaster recovery on virtual machines by enabling replication via Azure Site Recovery.
2. **Description**: This policy ensures that virtual machines have disaster recovery configurations enabled via Azure Site Recovery. Virtual machines without disaster recovery configurations are vulnerable to outages and other disruptions. The policy initiates replication using preset configurations to facilitate business continuity.
3. **Scope**: Apply this policy to Production Virtual Machines, platinum or gold\_silver applications.
4. **Settings**: **Tag-based Assignment**: Configure the policy to apply only to machines with a specific tag. This ensures that only specific servers with a requirement for Azure Site Recovery are affected.
5. **Configuration Steps**: a. **Access Azure Policy**: Log in to the Azure portal (<https://portal.azure.com/>) using appropriate credentials.

b. **Navigate to Azure Policy**: In the Azure portal, navigate to the Azure Policy service.

c. **Create a New Policy Definition**:

* + Click on "Definitions" and then "New Policy Definition".
  + Enter the policy name: "Configure disaster recovery on virtual machines".
  + Add a description explaining the purpose of the policy.
  + Configure the policy rules:
    - Set the policy rule to enable replication via Azure Site Recovery.
    - Define the conditions for the policy, such as only applying to Production Virtual Machines.
    - Optionally, set up tag-based assignment to apply the policy only to specific machines with a designated tag.

d. **Assign the Policy**:

* + After defining the policy, click on "Assignments" and then "Assign policy".
  + Select the scope where the policy will be applied (Subscription, Resource Group, or Management Group).
  + Review and confirm the assignment details.

1. **Testing and Validation**:
   * Once the policy is assigned, verify its enforcement on the designated virtual machines.
   * Test the policy by creating new virtual machines and ensuring that the disaster recovery configurations are automatically enabled according to the policy rules.
2. **Monitoring and Maintenance**:
   * Regularly monitor compliance with the policy to ensure that all Production Virtual Machines have disaster recovery configurations enabled.
   * Periodically audit and review the policy's effectiveness in maintaining disaster recovery readiness for virtual machines.

# Configuration Templates

The following configuration template varies slightly from other documents. The below shows how to configure the Azure Policy recommended to enable ASR on Virtual Machines.

## Azure Policy Settings

|  |  |
| --- | --- |
| Policy Parameter | Setting |
| **Scope** | The Management Group, Subscription, or Resource Group that the Policy is assigned to. |
| **Exclusions** | Any Management Group, Subscription, or Resource Group required to be exempted from the policy |
| **Source Region** | Australia Southeast |
| **Target Region** | Australia East |
| **Target Resource Group** | The resource group that will host the Virtual Machine that will be created in the Disaster Recovery region |
| **Vault Resource Group** | The resource group that hosts the Recovery Services vault to be used for a given deployment |
| **Recovery Service Vault** | The name of the Recovery Services Vault supporting ASR for a given deployment |
| **Remediation** | Check the box to Create a remediation task |
| **Managed Identity** | Check the box to create a Managed Identity |
| **Type of Managed Identity** | System Assigned |
| **Managed Identity Location** | Australia Southeast |
| **Tag Type** | Inclusion |
| **Tag Name** | ASR\_Enabled\_Platinum  or  ASR\_Enabled\_GoldSilver |
| **Tag Value** | Yes |

## Platinum Retention Policy Settings

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | Platinum\_ASR\_RetentionPolicy |
| **Retention Period (in days)** | 15 |
| **App Consistent Snapshots (hours)** | 4 |
| **Automation Account** | aa-prd-auea-[appname]-asr-01 |

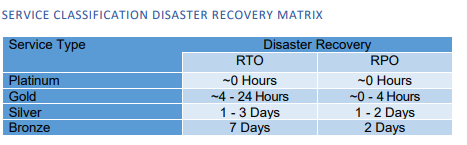
## Gold/Silver Retention Policy Settings

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | GoldSIlver\_ASR\_RetentionPolicy |
| **Retention Period (in days)** | 7 |
| **App Consistent Snapshots (hours)** | 8 |
| **Automation Account** | aa-prd-auea-[appname]-asr-01 |

Ensure to replace placeholders like [appname] with actual application names or appropriate values as required in the environment.

[Also paste screenshot of the deployment here]

## RTO and RPO matrix



Ensure to replace placeholders like [appname] with actual application names or appropriate values as required in the environment.

[Also paste screenshot of the deployment here]

# 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 | Arshdeep Singh |
| Position | Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-gb/pricing/details/site-recovery/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-4)