**CORE SERVICE DESIGN:**

**Azure Files**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Files Core Service Design |
| **File Name** | Ambulance Victoria – Azure Files Core Service Design v3.0.docx |
| **Version** | 3.0 |
| **Status** | Updated |
| **Release Date** | 29/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 22/02/2024 |
| 2.0 | Updated | Minor feedback | 12, 13 | 28/02/2024 |
| 3.0 | Updated | Platinum only service | 7, 16, 18 | 29/02/2024 |

Table of Contents

[1. Overview 5](#_Toc159503923)

[1.1 Purpose and Audience 5](#_Toc159503924)

[1.2 Scope and Key Deliverables 5](#_Toc159503925)

[1.3 Glossary and Definitions 6](#_Toc159503926)

[2. Executive Summary 7](#_Toc159503927)

[3. Resource Cost 8](#_Toc159503928)

[4. WAF and Security Control Alignment 8](#_Toc159503929)

[4.1 Reliability 9](#_Toc159503930)

[4.1.1 Overview 9](#_Toc159503931)

[4.1.2 Azure Files Reliability Checklist 9](#_Toc159503932)

[4.2 Cost Optimisation 9](#_Toc159503933)

[4.2.1 Overview 9](#_Toc159503934)

[4.2.2 Azure Files Cost Optimisation Checklist 9](#_Toc159503935)

[4.3 Operational Excellence 10](#_Toc159503936)

[4.3.1 Overview 10](#_Toc159503937)

[4.3.2 Azure Files Operational Excellence Checklist 10](#_Toc159503938)

[4.4 Performance Efficiency 10](#_Toc159503939)

[4.4.1 Overview 10](#_Toc159503940)

[4.4.2 Azure Files Performance Efficiency Checklist 10](#_Toc159503941)

[4.5 Security 11](#_Toc159503942)

[4.5.1 Overview 11](#_Toc159503943)

[5. Architecture Summary 12](#_Toc159503944)

[5.1 Resource Overview 12](#_Toc159503945)

[5.1.1 Azure File Sync 12](#_Toc159503946)

[5.2 RBAC 12](#_Toc159503947)

[5.3 Design Decisions and Justifications 13](#_Toc159503948)

[5.3.1 File Share Protocol 13](#_Toc159503949)

[5.3.2 Large File Shares 13](#_Toc159503950)

[5.3.3 File Share Type 14](#_Toc159503951)

[5.3.4 Network Connectivity 14](#_Toc159503952)

[5.3.5 Secure Transfer 14](#_Toc159503953)

[5.3.6 Encryption 15](#_Toc159503954)

[5.3.7 Authentication 15](#_Toc159503955)

[5.3.8 Threat Protection 15](#_Toc159503956)

[5.3.9 Redundancy 15](#_Toc159503957)

[5.3.10 Soft Delete 16](#_Toc159503958)

[5.3.11 Backup 16](#_Toc159503959)

[5.3.12 Logging 16](#_Toc159503960)

[6. Azure Policies 17](#_Toc159503961)

[7. Configuration Templates 17](#_Toc159503962)

[7.1 Primary Platinum File Share 17](#_Toc159503963)

[7.2 Secondary Platinum File Share 17](#_Toc159503964)

[7.3 Primary Gold/Silver File Share 18](#_Toc159503965)

[7.4 Primary Bronze File Share 18](#_Toc159503966)

[8. Acceptance 19](#_Toc159503967)

# Overview

This document covers the baseline design for the Azure Files 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 Files 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 Files.

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 Files 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 : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure Files 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.

File Services are assumed to always be a Platinum service, so there are no differences between service tier settings.

For this service the main baseline configurations include:

* SMB is preferred over NFS to be used where possible and is assumed the standard.
* Secure Transfer will remain enabled unless disabling cannot be avoided (for NFS shares)
* Public connectivity will be disabled, and private endpoints will be used.
* Microsoft Defender for Storage will be enabled.
* Geo-redundancy will be enabled.
* Soft delete will be enabled with the following settings:
  + Platinum – snapshot every 4 hours with 30-day retention

Note that most of the Well Architected Framework guidance applies to the Storage Account hosting the Azure Files instance which has been covered in a separate design document.

# Resource Cost

The following is the resource pricing construct for Azure Files assuming Geo-redundancy:

|  |  |  |  |
| --- | --- | --- | --- |
| Data storage | Transaction optimized | Hot | Cool |
| **Data at-rest (GiB/month)**  Per GiB storage costs for a file’s data stream. | **$0.1669** per used GiB | **$0.0838** per used GiB | **$0.0683** per used GiB |
| **Snapshots (GiB/month)**  Snapshot pricing covers additional storage cost of differential snapshots. | **$0.1669** per used GiB | **$0.0838** per used GiB | **$0.0683** per used GiB |
| **Metadata at-rest (GiB/month)**  The cost of file system metadata associated with files and directories such as access control lists (ACLs) or other properties. | Included | **$0.087** | **$0.087** |

Table : Pricing construct for Azure File Shares

# 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[[2]](#footnote-3). 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 Files Reliability Checklist

There is no Reliability guidance for Azure Files under the Well Architected Framework. For details around Reliability with respect to the Storage Account please refer to the Storage Account and Blob Core Service Design document.

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[3]](#footnote-4). 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 Files Cost Optimisation Checklist

There is no Cost Optimisation guidance for Azure Files under the Well Architected Framework. For details around Cost Optimisation with respect to the Storage Account please refer to the Storage Account and Blob Core Service Design document.

## 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 Files Operational Excellence Checklist

There is no Operational Excellence guidance for Azure Files under the Well Architected Framework. For details around Cost Optimisation with respect to the Storage Account please refer to the Storage Account and Blob Core Service Design document.

## 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[[4]](#footnote-5). This covers capacity and scalability:

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

### Azure Files Performance Efficiency Checklist

There is no Performance Efficiency guidance for Azure Files under the Well Architected Framework. For details around Performance Efficiency with respect to the Storage Account please refer to the Storage Account and Blob Core Service Design document.

## 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[[5]](#footnote-6):

* 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 applicable:

* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* DP-3: Encrypt sensitive data in transit
* DP-4: Encrypt sensitive data at rest
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Architecture Summary

## Resource Overview

Azure Files is a fully managed file share service that is accessible via industry standard protocols such as Server Message Block (SMB) and Network File System (NFS). Azure file shares can be mounted concurrently with cloud or on-prem deployments[[6]](#footnote-7).

The SMB shares are accessible from multiple OS clients: Windows, Linux, and macOS. NFS shares are accessible from Linux clients.

Azure File shares can be used in several common scenarios:

* Replace or uplift on-prem file servers
* Lift and shift applications
* Simplify cloud development
  + Applications having a central location for loading configurations
  + Diagnostic sharing through mounting files
  + Testing and debugging with a file share locally allows access to tools rapidly
* Containerisation by offering persistent volumes for stateful containers.

Broadly speaking there are two options for implementing Azure Files[[7]](#footnote-8):

* Direct mounting – servers mount the Azure File share using SMB or NFS
* Cache Azure File through Azure File Sync – this allows you to centralise file shares in Azure Files whilst maintaining an On-Prem file server

Note that unlike Blob Storage, lifecycle management policies are not applicable to file shares.

### Azure File Sync

Azure File Sync allows you to centralise file shares in Azure Files, whilst keeping the compatibility of an on-prem file server. It essentially transforms a Windows Server into a quick cache of the file share.

It allows you to cache Azure File shares on an On-Prem server or another cloud VM.

## RBAC

For Azure Files the following roles can be applied[[8]](#footnote-9):

|  |  |
| --- | --- |
| Role Name | Description |
| Storage File Data Privileged Contributor | Allows for read, write, delete, and modify ACLs on files/directories in Azure file shares by overriding existing ACLs/NTFS permissions. This role has no built-in equivalent on Windows file servers. |
| Storage File Data Privileged Reader | Allows for read access on files/directories in Azure file shares by overriding existing ACLs/NTFS permissions. This role has no built-in equivalent on Windows file servers. |
| Storage File Data SMB Share Contributor | Allows for read, write, and delete access on files/directories in Azure file shares. This role has no built-in equivalent on Windows file servers. |
| Storage File Data SMB Share Elevated Contributor | Allows for read, write, delete, and modify ACLs on files/directories in Azure file shares. This role is equivalent to a file share ACL of change on Windows file servers. |
| Storage File Data SMB Share Reader | Allows for read access on files/directories in Azure file shares. This role is equivalent to a file share ACL of read on Windows file servers. |

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 Azure Files 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.

### File Share Protocol

**Design Reference:** N/A

**Design Decision:** Use SMB over NFS where possible. Use the latest version that is compatible with the application or use case.

**Design Justification:** SMB allows you to utilise security and operational features such as encryption in transit, Azure File Sync, AzCopy and Azure Storage Explorer[[9]](#footnote-10). As such it is recommended to use SMB shares over NFS unless there is a specific requirement that cannot be met such as POSIX controls and UNIX permissions. SMB can also be used for Windows, Linux, and macOS clients, where NFS is only compatible with Linux.

### Large File Shares

**Design Reference:** N/A

**Design Decision:** Large File Shares will not be enabled by default.

**Design Justification:** Large File Shares should only be enabled as required. For most applications and use cases the 5TiB limit will not be met, so is unnecessary to enabled. Additionally, it introduces some limitations such as Geo-Redundancy cannot be enabled (though it is in public preview), only Locally-Redundant is currently supported for Large File Shares.

### File Share Type

**Design Reference:** N/A

**Design Decision:** Standard file shares with GRS redundancy will be used for Azure Files deployments.

**Design Justification:** Standard file shares are recommended for most scenarios. Premium should be used only if there is a specific requirement from an application design that requires extremely low latency, large IOPS, or extremely fast data transfer speed.

### Network Connectivity

**Design Reference:** Microsoft Security Benchmark [NS-1](#_Azure_Files_Security)

**Design Decision**: ensure that port 445 is open and controlled via Firewall and NSGs for access to SMB file shares. Public connectivity will be disabled, and a Private Endpoint will be used.

**Design Justification**: Port 445 in some cases may be blocked due to legacy security concerns about previous versions of SMB protocols. It can be allowed through Firewall and NSGs for security purposes.

Connectivity to the storage account and the file share will be controlled with Private Endpoints as this is the most secure form of connectivity. Public endpoints will be disabled. If it is not possible to use Private Endpoints, then public access should still be disabled, and the storage account firewall itself should be used to only allow specific traffic from specific IP ranges through.

### Secure Transfer

**Design Reference:** Microsoft Security Benchmark [DP-3](#_Azure_Files_Security)

**Design Decision:** Secure transfer is required by default for Azure storage accounts and will be left enabled by default.

**Design Justification:** Disabling secure transfer will allow unencrypted traffic through. This is not recommended so the default will be left as is. Note that NFS file shares don’t support an encryption mechanism, so it is a requirement to disable secure transfer if NFS file shares are required.

### Encryption

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

**Design Decision:** Encryption in transit is enabled by default and will not be disabled. This means that all versions of SMB will be allowed, except for SMB 2.1. Additionally, TLS 1.2 will be set as the minimum.

**Design Justification:** Note that encryption in transit is not supported for NFS share types, so again it is preferable to use SMB if the application allows for this. Encryption at rest is deployed by default on Azure Storage Accounts for files.

### Authentication

**Design Reference:** Microsoft Security Benchmark [IM-1](#_Overview)

**Design Decision:** Microsoft Entra ID (Azure AD) authentication will be used as the default. If required for Hybrid connectivity, Kerberos authentication can be enabled on a File Share level.

**Design Justification:** Using Microsoft Entra ID as the central, and native, authentication mechanism is the most secure as it can be used to require MFA. If Kerberos is required it does not support using MFA to access Azure File shares configured with Microsoft Entra Kerberos, so the storage account will need to be exempted from MFA if access is required in this way.

### Threat Protection

**Design Reference:** Microsoft Security Benchmark [LT-1](#_Azure_Files_Security)

**Design Decision:** Microsoft Defender for Storage will be enabled.

**Design Justification:** Threat protection will assist in early identification of malicious behaviour on Storage Accounts. It will continuously monitor the storage account for any such behaviour and provide recommendations on how to bolster security.

### Redundancy

**Design Reference:** N/A

**Design Decision:** Geo-redundancy will be enabled on Platinum and critical workloads. Locally redundant will be used for Bronze or Non-Production workloads.

**Design Justification:** Geo-redundancy is required to secure Platinum data and ensure that it can be recovered in case of a persistent regional outage. It is not required for Non-Production workloads which can sufficiently be covered with Locally Redundant replication.

### Soft Delete

**Design Reference:** N/A

**Design Decision:** Soft delete will be enabled for Azure Files deployments.

**Design Justification:** Soft delete protects against accidental deletions and allows the File share to be recoverable. It is recommended to have Platinum file shares be recoverable for 30 days.

### Backup

**Design Reference:** Microsoft Security Benchmark [BR-1](#_Overview)

**Design Decision:** Azure File shares will be backed up using the native Azure Backup mechanic until such time that an alternative (e.g. Commvault) is put in place.

**Design Justification:** It is a security and compliance requirement to ensure that recovery points can be met. This can be achieved using Azure Backup.

**Design Details:** For Platinum deployments hourly backups will take place every 4 hours and be retained for 30 days.

### Logging

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Overview)

**Design Decision:** Logging will be enabled on the file share level and sent to the central log analytics workspace in that region.

**Design Justification:** It is a security requirement to capture logs that can assist with identifying malicious behaviour in the environment. AllLogs and Transaction metrics will be captured and cent to the central workspace for that region.

# Azure Policies

There are no Azure Policies required to support this service.

# Configuration Templates

## Primary Platinum File Share

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | share-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Tier** | Transaction Optimised |
| **Protocol** | SMB |
| **Backup** | Enabled |
| **Large File Shares** | Disabled |
| **Maximum Capacity** | 5 TiB |
| **Redundancy** | Geo-redundant |
| **Backup Policy Name** | backupfile\_platinum |
| **Backup Frequency** | Every 4 hours |
| **Backup retention** | 30 days |

## Secondary Platinum File Share

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | share-dr-auea-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Tier** | Transaction Optimised |
| **Protocol** | SMB |
| **Backup** | Enabled |
| **Large File Shares** | Disabled |
| **Maximum Capacity** | 5 TiB |
| **Redundancy** | Locally redundant |
| **Backup Policy Name** | backupfile\_platinum\_dr |
| **Backup Frequency** | Every 4 hours |
| **Backup retention** | 30 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 | 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://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/storage/files/storage-files-planning [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/storage/files/files-nfs-protocol [↑](#footnote-ref-10)