**CORE SERVICE DESIGN:**

**Azure Bastion**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Bastion Core Service Design |
| **File Name** | Ambulance Victoria – Azure Bastion Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 18/01/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 18/01/2024 |
| 2.0 | Updated | Minor feedback | 14, 15 | 24/01/2024 |

Table of Contents

[1. Overview 5](#_Toc156486110)

[1.1 Purpose and Audience 5](#_Toc156486111)

[1.2 Scope and Key Deliverables 5](#_Toc156486112)

[1.3 Glossary and Definitions 6](#_Toc156486113)

[2. Executive Summary 7](#_Toc156486114)

[3. Resource Cost 7](#_Toc156486115)

[4. WAF and Security Control Alignment 8](#_Toc156486116)

[4.1 Reliability 8](#_Toc156486117)

[4.1.1 Overview 8](#_Toc156486118)

[4.1.2 Azure Bastion Reliability Checklist 8](#_Toc156486119)

[4.2 Cost Optimisation 9](#_Toc156486120)

[4.2.1 Overview 9](#_Toc156486121)

[4.2.2 Azure Bastion Cost Optimisation Checklist 9](#_Toc156486122)

[4.3 Operational Excellence 9](#_Toc156486123)

[4.3.1 Overview 9](#_Toc156486124)

[4.3.2 Azure Bastion Operational Excellence Checklist 9](#_Toc156486125)

[4.4 Performance Efficiency 10](#_Toc156486126)

[4.4.1 Overview 10](#_Toc156486127)

[4.4.2 Azure Bastion Performance Efficiency Checklist 10](#_Toc156486128)

[4.5 Security 11](#_Toc156486129)

[4.5.1 Overview 11](#_Toc156486130)

[4.5.2 Azure Bastion Security Checklist 11](#_Toc156486131)

[5. Architecture Summary 12](#_Toc156486132)

[5.1 Resource Overview 12](#_Toc156486133)

[5.2 RBAC 13](#_Toc156486134)

[5.3 Solution Diagram 14](#_Toc156486135)

[5.4 Design Decisions and Justifications 14](#_Toc156486136)

[5.4.1 Azure Bastion SKU Selection 14](#_Toc156486137)

[5.4.2 Use Bastion for administrative purposes 15](#_Toc156486138)

[5.4.3 Network Segmentation 15](#_Toc156486139)

[5.4.4 Securely manage credentials and secrets 15](#_Toc156486140)

[5.4.5 Follow the principle of Least Privilege 15](#_Toc156486141)

[5.4.6 Logging and threat detection 16](#_Toc156486142)

[6. Azure Policies 16](#_Toc156486143)

[7. Configuration Templates 17](#_Toc156486144)

[7.1 Primary Region Bastion 17](#_Toc156486145)

[7.2 DR Region Bastion 18](#_Toc156486146)

[8. Acceptance 19](#_Toc156486147)

# Overview

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

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 Bastion 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 Bastion 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:

* There is no distinction between service tiers for Azure Bastion. It will be deployed centrally and manage all application landing zones.
* An NSG with specific rules for Bastion must be attached to the AzureBastionSubnet
* The Standard SKU will be used for its enhanced security and feature set.
* Logs will be sent to the central Log Analytics workspace.

# Resource Cost

|  |  |
| --- | --- |
| SKU Pricing | Cost |
| Basic SKU | $0.278 per hour |
| Standard SKU | $0.424 per hour (2 instances included) |
| Additional Standard Instances | $0.205 per hour (above 2 instances) |
| **Outbound Data Transfer Pricing** | **Cost** |
| First 5GB/month | Free |
| 5GB – 10TB/month | $0.1752 per GB |
| Next 40 TB/month | $0.1241 per GB |
| Next 100 TB/month | $0.1198 per GB |
| Next 350 TB/month | $0.1168 per GB |
| Over 500 TB/month | Contact Microsoft for details |

Table 2: Pricing Construct[[2]](#footnote-3)

# 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 Bastion Reliability Checklist

Note that there is no specific guidance in Azure’s Well Architected Framework for Reliability for Azure Bastion.

## 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 Bastion Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Configure Azure Bastion for operational access | Yes | Yes | IaC – already deployed | At deployment |

Table 3: 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

### Azure Bastion Operational Excellence Checklist

Note that there is no specific guidance in Azure’s Well Architected Framework for Operational Excellence for Azure Bastion.

## 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 Bastion Performance Efficiency Checklist

Note that there is no specific guidance in Azure’s Well Architected Framework for Performance Efficiency for Azure Bastion.

## 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 applicable to Azure Bastion:

* NS-1: Establish network segmentation boundaries
* IM-8: Restrict the exposure of credential and secrets
* PA-7: Follow just enough administration (least privilege) principle
* DP-3: Encrypt sensitive data in transit
* DP-6: Use a secure key management process
* LT-4: Enable logging for security investigation

### Azure Bastion Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 3.2.4 | Administrative activities are conducted through jump servers. | Yes | Yes | Already deployed - Bastion | Operational |

Table 4: Security checklist summary

# Architecture Summary

## Resource Overview

Azure Bastion is an Azure Native PaaS tool that manages SSH and RDP access to servers[[7]](#footnote-8). It makes use of secure protocols (HTML5, TLS on port 443, and no support for versions of TLS earlier than 1.2). VMs can be accessed without them requiring a Public IP address. The implication of this is that VMs are protected from port scanning as they do not need to be exposed to the Internet. Microsoft constantly updates the service to keep it hardened against Zero-Day exploits.

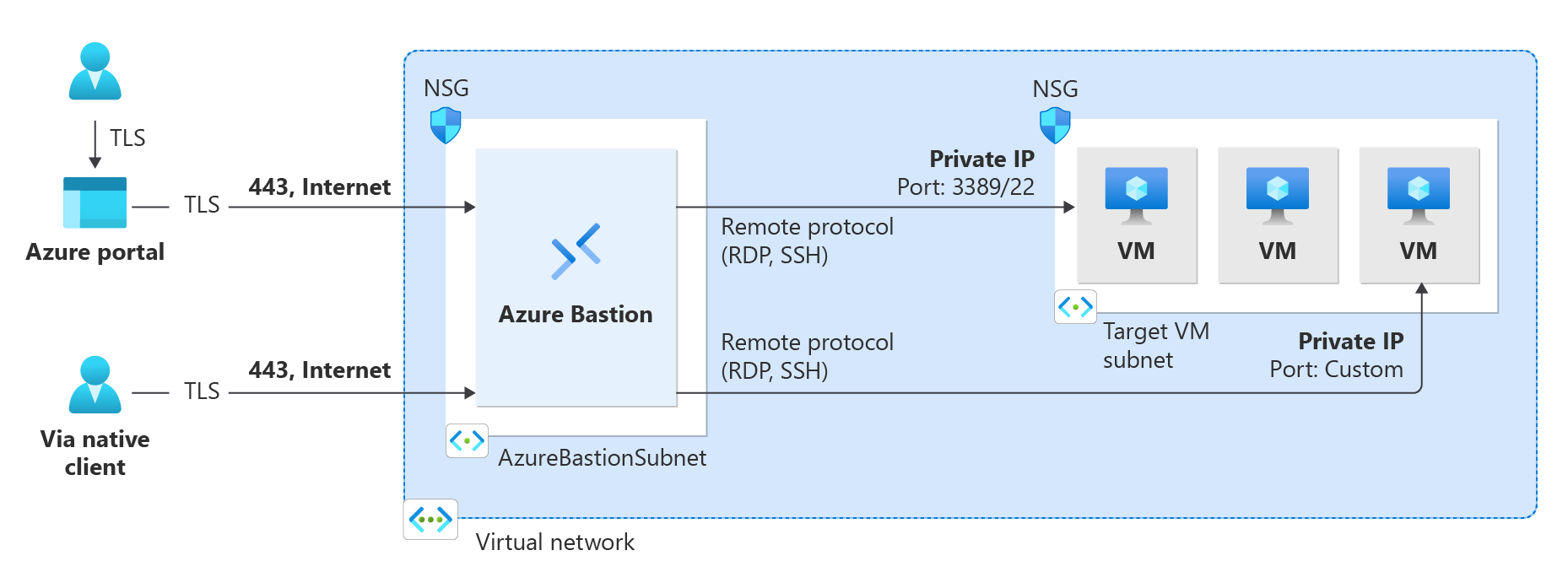


Figure 1: Diagram of users connecting to Virtual Machines via Bastion

To deploy Azure Bastion, the minimum subnet size is /26 to allow for scaling. The subnet must be called AzureBastionSubnet and cannot contain any other resources. For a hub-and-spoke topology, Bastion is only required to be deployed to the hub and will be able to reach Virtual Machines in the spoke virtual networks if they are peered to the hub that hosts the Bastion instance[[8]](#footnote-9).

The following shows a comparison of Azure Bastion SKUs available. Note there is also a Developer SKU that is currently in Preview in a limited number of regions, so it is not considered for this design[[9]](#footnote-10):

|  |  |  |
| --- | --- | --- |
| Feature | Basic SKU | Standard SKU |
| Connect to target VMs in same virtual network | Yes | Yes |
| Connect to target VMs in peered virtual networks | [Yes](https://learn.microsoft.com/en-us/azure/bastion/vnet-peering) | [Yes](https://learn.microsoft.com/en-us/azure/bastion/vnet-peering) |
| Support for concurrent connections | Yes | Yes |
| Access Linux VM Private Keys in Azure Key Vault (AKV) | Yes | Yes |
| Connect to Linux VM using SSH | [Yes](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-ssh-linux) | [Yes](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-ssh-linux) |
| Connect to Windows VM using RDP | [Yes](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows) | [Yes](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows) |
| Connect to Linux VM using RDP | No | Yes |
| Connect to Windows VM using SSH | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-ssh-windows) |
| Specify custom inbound port | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#ports) |
| Connect to VMs using Azure CLI | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/native-client) |
| Host scaling | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#instance) |
| Upload or download files | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/vm-upload-download-native) |
| Kerberos authentication | [Yes](https://learn.microsoft.com/en-us/azure/bastion/kerberos-authentication-portal) | [Yes](https://learn.microsoft.com/en-us/azure/bastion/kerberos-authentication-portal) |
| Shareable link | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/shareable-link) |
| Connect to VMs via IP address | No | [Yes](https://learn.microsoft.com/en-us/azure/bastion/connect-ip-address) |
| VM audio output | Yes | Yes |
| Disable copy/paste (web-based clients) | No | Yes |

Table 5: Comparison of Bastion SKU Features

## RBAC

The Reader role must be applied to the various target resources to allow the user access to the target VM. If the user does not have the Reader role on all the required resources, they will not be able to access the machine:

|  |  |  |
| --- | --- | --- |
| Role Name | Description | Target Resource |
| Reader | Grants user Read access to the Target Resource | Virtual Machine |
| Reader | Grants user Read access to the Target Resource | NIC attached to Virtual Machine |
| Reader | Grants user Read access to the Target Resource | Bastion |

Table 6: RBAC roles relevant for this core service

## Solution Diagram



Figure 2: Centralised Azure Bastion deployment in Hub-and-Spoke topology

## 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 Bastion 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.

### Azure Bastion SKU Selection

**Design Reference:** N/A

**Design Decision:** The Standard SKU of Bastion will be used.

**Design Justification:** The Standard SKU has enhanced features that makes connectivity to Virtual Machines even more secure. It allows you to disable copy/paste for web-based clients and has Host Scaling. It also supports RDP to Linux and SSH to Windows VMs to enhance the user experience, which is not available in the Basic SKU. Furthermore, the Standard SKU allows you to connect to Virtual Machines via IP address directly, which means the users are able to specify machines On-Premise to connect to. Note that this functionality is dependent on other factors such as routing, but this is a desired future state configuration. This is useful as it allows the transition to Cloud to become smoother by providing a single interface for RDP or SSH connectivity.

### Use Bastion for administrative purposes

**Design Reference:** Table 3 – [CO1](#_Azure_Bastion_Cost), Table 4 – [S1](#_Azure_Bastion_Security)

**Design Decision**: Bastion will be used for administrative duties for Azure Virtual Machines.

**Design Justification**: Bastion is a native PaaS solution, meaning that it is constantly updated and hardened by Microsoft, so is inherently secure. It should be used as the primary tool for RDP/SSH to Virtual Machines. If an IaaS Jumpbox is required, due to some tooling or application requirements, Azure Bastion should still be used to remote onto the Jumpbox itself.

Note that each Bastion deployment of the Standard SKU can support 20 concurrent RDP sessions and 40 concurrent SSH sessions for medium workloads (less for more data intensive workloads)[[10]](#footnote-11). The instances are created in the AzureBastionSubnet. The minimum recommended size for the subnet is /26 to allow for this scaling to take place.

The default deployment will use two instances per Bastion host, but this can be increased as required.

### Network Segmentation

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

**Design Decision:** Bastion will be deployed in a virtual network in a subnet that is a minimum /26. NSGs will be used to allow Bastion control of Azure Virtual Machines.

**Design Justification:** to ensure that Bastion can appropriately manage Virtual Machines, a specific set of rules are required on the Bastion subnet[[11]](#footnote-12).Additionally, the subnet that hosts the target Virtual Machine should also RDP or SSH ports through. These requirements are detailed in the [Configuration Templates](#_Configuration_Templates) section.

### Securely manage credentials and secrets

**Design Reference:** Microsoft Security Benchmark [IM-8, DP-6](#_Azure_Bastion_Security)

**Design Decision:** If SSH Keys are used for access to machines via Bastion, the keys should be stored securely in an Azure Key Vault.

**Design Justification:** It is a security risk to store secrets and keys in a users’ local environment or to have them hard coded in various places. As such, a secure solution, in this case the native Azure Key Vault service, should be used to store any SSH keys required to access a server through Azure Bastion.

### Follow the principle of Least Privilege

**Design Reference:** Microsoft Security Benchmark [PA-7](#_Azure_Bastion_Security)

**Design Decision:** RBAC will be used to control access to servers. Note that two sets of RBAC are required – access to Bastion as well as access on the target server.

**Design Justification:** RBAC should always be used to control Least Privilege access to resources. Else users will have no access, so it must be granted specifically to allow access.

**Design Details:**

The service itself doesn’t understand the concept of RBAC for access, however the user must have the following applied to access the target machine[[12]](#footnote-13):

* Reader role on the target virtual machine
* Reader role on the NIC with the private IP of the target virtual machine
* Reader role on the Azure Bastion resource

### Logging and threat detection

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

**Design Decision:** Resource Logs will be enabled for Azure Bastion.

**Design Justification:** Bastion resource logs track metrics such as remote sessions and logons. This is required to audit any security breaches and track last accesses to servers that may have been compromised or changed without proper processes having been followed.

**Design Details:** allLogs and AllMetrics will be configured to be sent to the relevant Log Analytics workspace within that region.

# Azure Policies

The only required exemption to standard policies is for the Deny Public IP Policy to be removed so that the Public IP for Bastion can be deployed. Note that this is already in place based on the current deployment.

# Configuration Templates

There are no differences in the deployment of Bastion between Service Tiers. It is assumed to be a Platinum service and is centralised in the Connectivity subscription.

## Primary Region Bastion

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Subscription | AV ALZ Connectivity |
| Resource Group | rg-prd-ause-connectivity-01 |
| Name | bas-prd-ause-hub-01 |
| Tier | Standard |
| Instance Count | 2 |
| Kerberos Authentication | Not enabled |
| Copy and Paste | Enabled |
| Native client support | Enabled |
| IP based connection | Not enabled (enable if connecting to On-Premise machines is required) |
| Shareable Link | Not enabled (enable if required to share link to new users or guest accounts) |
| Virtual Network | vnet-prd-ause-hub-01 |
| Subnet | AzureBastionSubnet (10.253.18.0/24) |
| **Public IP Configuration** |  |
| Public IP Name | pip-prd-ause-bas-01 |
| SKU | Standard |
| Tier | Regional |
| Assignment | Static |
| Routing Preference | Microsoft Network |
| **Diagnostic Settings** |  |
| Logs to be collected | allLogs  AllMetrics |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |

## DR Region Bastion

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Subscription | AV ALZ Connectivity |
| Resource Group | rg-prd-auea-connectivity-01 |
| Name | bas-prd-auea-hub-01 |
| Tier | Standard |
| Instance Count | 2 |
| Kerberos Authentication | Not enabled |
| Copy and Paste | Enabled |
| Native client support | Enabled |
| IP based connection | Not enabled (enable if connecting to On-Premise machines is required) |
| Shareable Link | Not enabled (enable if required to share link to new users or guest accounts) |
| Virtual Network | vnet-prd-auea-hub-01 |
| Subnet | AzureBastionSubnet (10.253.146.0/24) |
| **Public IP Configuration** |  |
| Public IP Name | pip-prd-auea-bas-01 |
| SKU | Standard |
| Tier | Regional |
| Assignment | Static |
| Routing Preference | Microsoft Network |
| **Diagnostic Settings** |  |
| Logs to be collected | allLogs  AllMetrics |
| Log Analytics Workspace | law-prd-auea-mgmt-01 |

# 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-bastion/ [↑](#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/bastion/bastion-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/bastion/vnet-peering [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/bastion/configuration-settings [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#instance [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-bastion-security-baseline [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-bastion-security-baseline [↑](#footnote-ref-13)