**CORE SERVICE DESIGN:**

**Defender for Servers**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Defender for Servers Core Service Design |
| **File Name** | Ambulance Victoria – Defender for Servers Core Service Design v1.0.docx |
| **Version** | 2.0 |
| **Status** | Draft |
| **Release Date** |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Draft | N/A | All | 15/05/2024 |

Table of Contents

[1. Overview 5](#_Toc167289518)

[1.1 Purpose and Audience 5](#_Toc167289519)

[1.2 Scope and Key Deliverables 5](#_Toc167289520)

[1.3 Glossary and Definitions 6](#_Toc167289521)

[2. Executive Summary 7](#_Toc167289522)

[3. Resource Cost 8](#_Toc167289523)

[4. Architecture Summary 9](#_Toc167289524)

[4.1 Resource Overview 9](#_Toc167289525)

[4.2 RBAC 9](#_Toc167289526)

[4.3 Design Decisions and Justifications 10](#_Toc167289527)

[4.3.1 Enabling Defender on all resources 10](#_Toc167289528)

[4.3.2 Deployment via Policy 10](#_Toc167289529)

[5. Azure Policies 11](#_Toc167289530)

[6. Implementation Steps:- 12](#_Toc167289531)

[6.1 Selecting a Defender for Server plan: - 12](#_Toc167289532)

[6.2 Using Azure policy to enable Defender for Servers on VM’s: - 13](#_Toc167289533)

[7. Configuration Template 14](#_Toc167289534)

[8. Defender Agent Deployment 14](#_Toc167289535)

[9. Automatic Deployment: - 15](#_Toc167289536)

[9.1.1 For Azure Servers: - 15](#_Toc167289537)

[9.1.2 For On premises or ARC Enabled Servers: - 15](#_Toc167289538)

[10. Monitor Agent deployment and remediating missing agents: - 16](#_Toc167289539)

[10.1.1 Using Azure Policy: - 16](#_Toc167289540)

[10.1.2 Using Defender for cloud recommendations: - 16](#_Toc167289541)

[11. Manually Remediate missing agent deployment: 17](#_Toc167289542)

[11.1.1 For Azure VMs:- 17](#_Toc167289543)

[11.1.2 For ARC enabled servers: - 17](#_Toc167289544)

[11.1.3 Manual Deployment Using VM Guest baseline: 17](#_Toc167289545)

[12. Acceptance 18](#_Toc167289546)

# Overview

This document covers the baseline design for the Defender for Servers 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 Defender for Servers 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 Defender for Servers.

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 Defender for Servers 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 Defender for Servers 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.

This feature dictates security across the environment across all resources, so it is assumed to always be a Platinum service. Some of the main configurations include:

* Defender for all resources including the Servers will be enabled across all subscriptions including Defender CSPM and ISM Defender for workloads.
* Azure Policy with user managed identity will be used to enforce Defender plans being enabled automatically across the board for all subscriptions.

<*User Managed Identity goes here and the RBAC scope details to be mentioned here*>

# Resource Cost

Defender for Cloud pricing varies depending on the underlying resource type. Typically, it is a per instance per unit of time pricing[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
| Resource Type | Resource | Price |
| Servers | Microsoft Defender for Servers Plan 1 | **$0.011**/Server/hour |
|  | Microsoft Defender for Servers Plan 2 | **$0.031**/Server/hour |
| Containers | Microsoft Defender for Containers | **$0.0144**/vCore/hour4 |
| Databases | Microsoft Defender for SQL on Azure-connected databases | **$0.032**/Instance/hour2 |
|  | Microsoft Defender for SQL outside Azure | **$0.023**/Instance/vCore/hour3 |
|  | Microsoft Defender for MySQL | **$0.032**/Instance/hour |
|  | Microsoft Defender for PostgreSQL | **$0.032**/Instance/hour |
|  | Microsoft Defender for MariaDB | **$0.031**/Instance/hour |
|  | Microsoft Defender for Azure Cosmos DB5 | **$0.0019** per 100 RU/S/hour |
| Storage | Microsoft Defender for Storage1 | **$0.0205** per storage account/hour6 |
|  | Malware Scanning7 (add-on to Defender for Storage) | **$0.230**/GB of data scanned |
| Service Layer | Microsoft Defender for App Service | **$0.031**/Instance/hour |
|  | Microsoft Defender for Key Vault | **$0.38**/Vault/month |
|  | Microsoft Defender for Resource Manager | **$7.70**/Subscription/month |

Table 2: Pricing construct for Defender for Cloud

Here is link to the Azure pricing for various Defender for Cloud services.

[Pricing - Microsoft Defender for Cloud | Microsoft Azure](https://azure.microsoft.com/en-au/pricing/details/defender-for-cloud/)

# Architecture Summary

## Resource Overview

Azure Defender for Servers is a feature within Azure Security Centre that helps protect Windows and Linux servers in Azure, on-premises using Azure ARC, and in other clouds.

It provides advanced threat protection against attacks, including zero-day vulnerabilities and malware, by leveraging Microsoft's extensive threat intelligence and security analytics.

Azure Defender for Servers continuously monitors servers for suspicious activity, performs behavioural analysis, and alerts administrators to potential threats, enabling them to respond quickly to mitigate risks.

It also provides recommendations for improving the security posture of servers, such as applying missing security updates and configuring security settings correctly.

Microsoft Defender for Servers extends protection to all Windows and Linux machines that run in Azure. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR) and other threat protection features.

## RBAC

The following roles can be applied to Defender for Servers:

|  |  |
| --- | --- |
| Role Name | Description |
| Security Admin | View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations. |
| Security Assessment Contributor | Lets you push assessments to Microsoft Defender for Cloud |
| Security Reader | View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes. |

Table 4: 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 Defender for Servers 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.

### Enabling Defender on all resources

**Design Decision**: All Defender plans will be enabled for each subscription. Plan 2 is to be enabled for Defender for Servers.

**Design Justification**: All available plans will be enabled for the Defender for Servers along with other services.

* Defender for App Service
* Defender for Databases
* Defender for Storage
* Defender for Containers
* Defender for Key Vault
* Defender for Resource manager
* Defender for APIs
* Defender for AKS <depending on the whether AKS is to be used>

### Deployment via Policy

**Design Decision:** Azure Policy will be used to enable Defender for Servers on subscriptions.

**Design Justification:** Using Azure Policy to ensure Defender is enabled on all servers on new subscriptions removes a manual step required to enable the plans on new subscriptions. It will automatically set the plans as each subscription is created.

# Azure Policies

The following Azure Policies will be applied via an initiative to enable Defender on subscriptions as they are created: The Initiative name available to use is (Azure Defender Policies For Cloud).

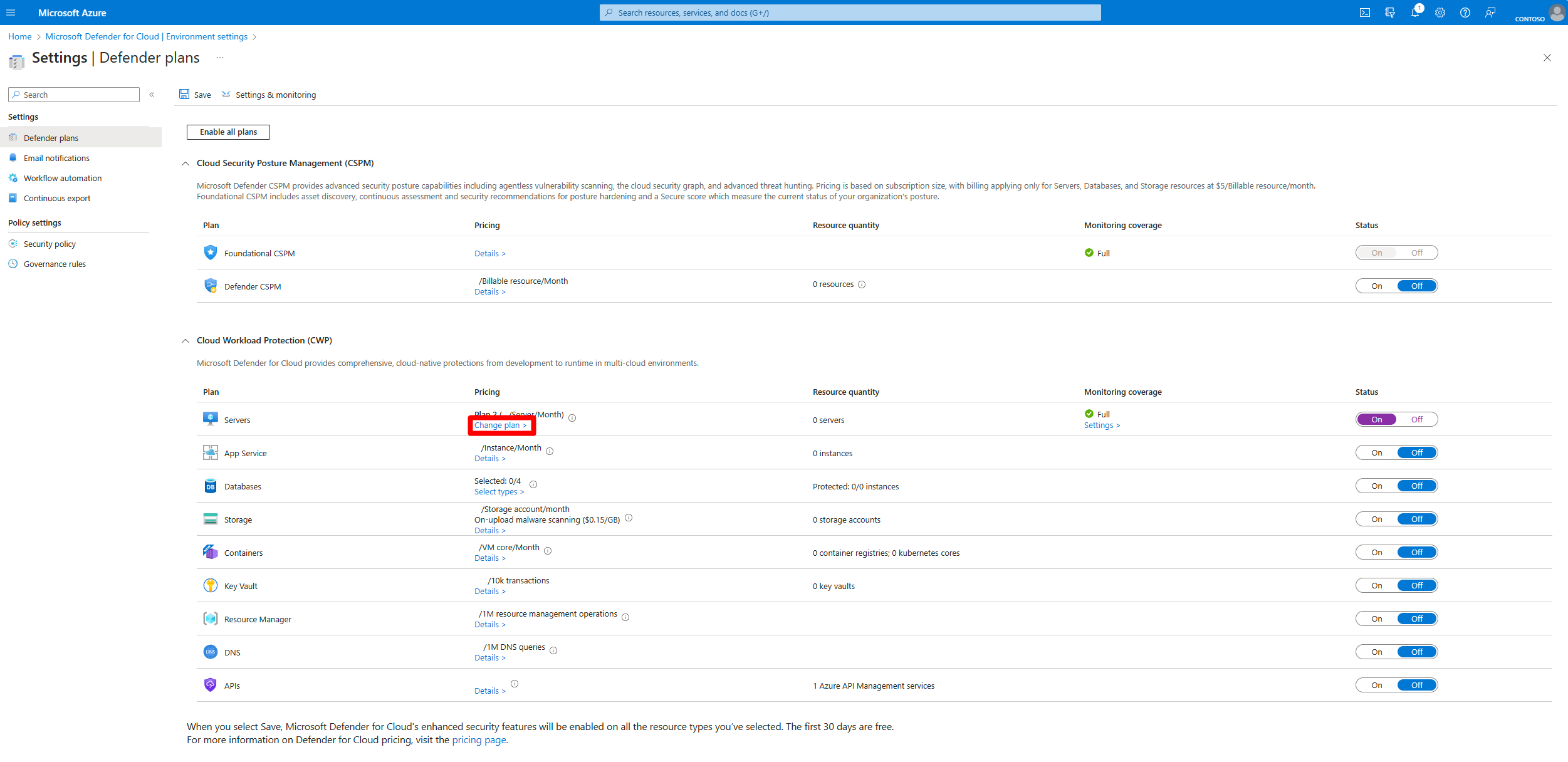
|  |  |
| --- | --- |
| Policy Name | Scope |
| Azure Defender for App Service should be enabled | av management group |
| Azure Defender for Azure SQL Database servers should be enabled | av management group |
| Azure Defender for Key Vault should be enabled | av management group |
| Azure Defender for open-source relational databases should be enabled | av management group |
| Azure Defender for Resource Manager should be enabled | av management group |
| **Azure Defender for servers should be enabled** | av management group |
| Azure Defender for SQL servers on machines should be enabled | av management group |
| Azure Defender for SQL should be enabled for unprotected Azure SQL servers | av management group |
| Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers | av management group |
| Azure Defender for SQL should be enabled for unprotected SQL Managed Instances | av management group |
| Azure Defender for Storage should be enabled | av management group |
| Azure Defender for Kubernetes should be enabled | av management group |
| Azure Defender for container registries should be enabled | av management group |

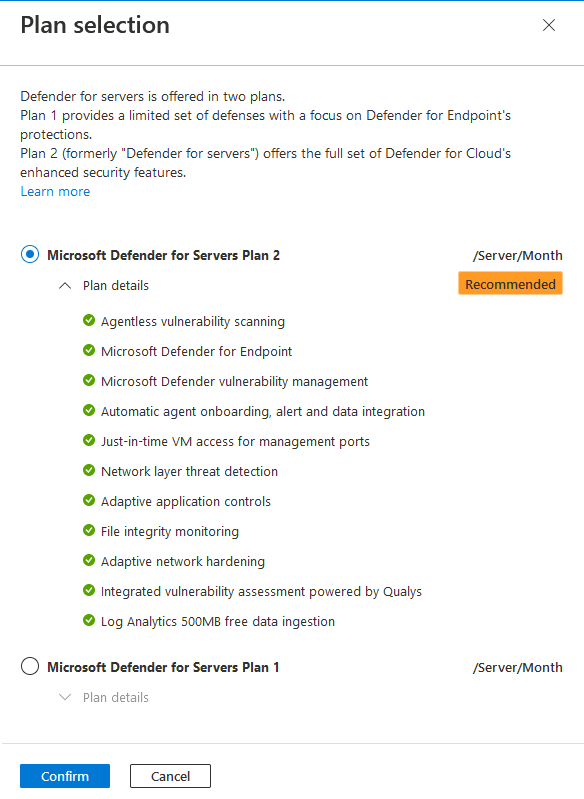
Table 5: Azure Policies

# Implementation Steps:-

# 6.1 Selecting a Defender for Server plan: -

When we enable the Defender for Servers plan, we're then given the option to select which plan - Plan 1 or Plan 2 - to enable. Plan 2 is to be enabled as per design decision and needs to be selected. As per screenshot below Enabled Defender plans for Servers including other services as per design decision. Plan 2 is to be selected after enabling Defender for Servers.



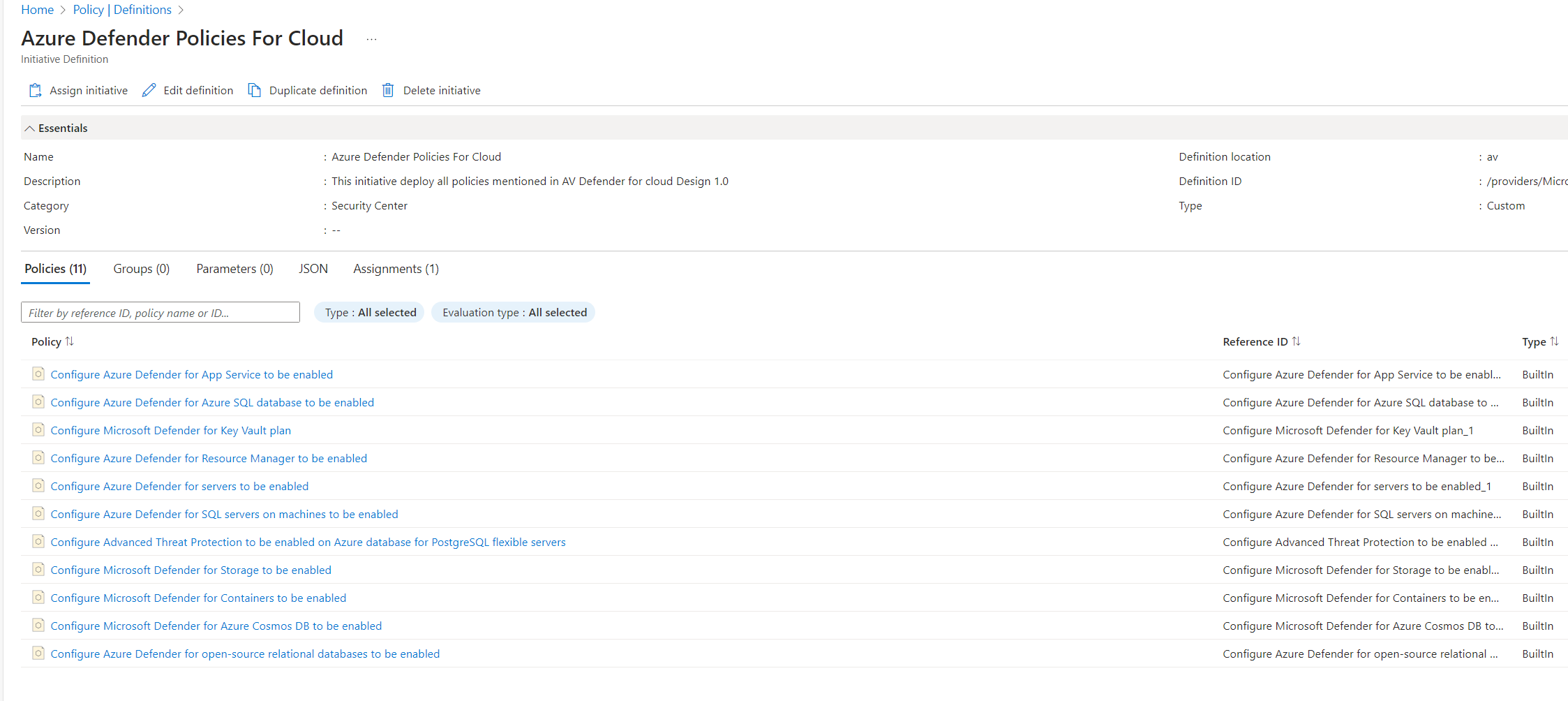


## 6.2 Using Azure policy to enable Defender for Servers on VM’s: -

We already have a built in Azure policy (Configure Azure Defender for servers to be enabled) which is combined and added to the initiative [Azure Defender Policies For Cloud].

Assigning this initiative to the AV management group (av management group) ensures that Defender is enabled for all servers in Azure.

Here is a screenshot of the Policy initiative: -



And here is a screengrab of Policy assignment: -

A screenshot of a computer

Description automatically generated

# Configuration Template

There is no specific configuration template for this deployment. The following table shows the list of plans that will be enabled for each new subscription:

|  |  |  |
| --- | --- | --- |
| Workload | Plan | Sub-components enabled |
| Servers | Plan 2 enabled | Agent deployment  Vulnerability Assessment  Endpoint Protection  Agentless scanning |
| App Service | N/A | N/A |
| Databases | SQL Databases  SQL server on machines  Open-source relational  Azure Cosmos DB | Azure Monitoring Agent for SQL server on machines |
| Storage | N/A | Malware scanning  Sensitive data discovery |
| Containers | N/A | Defender agent in Azure  Azure Policy for Kubernetees  Agentless discovery for Kubernetes  Agentless container vulnerability assessment |
| Key Vault | N/A | N/A |
| Resource Manager | N/A | N/A |
| APIs | Plan 1 | N/A |

# Defender Agent Deployment

Defender for Cloud collects data from Azure virtual machines (VMs) to monitor for security vulnerabilities and threats. Data is collected using the Azure Monitor Agent (AMA), which reads various security-related configurations and event logs from the machine and copies the data to the Log Analytics workspace for analysis. This agent is also required if the VMs are used by an Azure managed service such as Azure Kubernetes Service or Azure Service Fabric. Microsoft recommends configuring auto-provisioning to automatically deploy the agent. Along with the use of auto-provisioning, manually deploy the agent to any VMs in case they are missing the agent using the instructions in the remediation steps.

Azure Monitor Agent uses [data collection rules](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview), where we define which data we want each agent to collect. Data collection rules let us manage data collection settings at scale and define unique, scoped configurations for subsets of machines.

**To collect data using Azure Monitor Agent:**

1. Install the agent on the resource.
2. Define a data collection rule and associate the resource to the rule.

More details on the Azure monitor agent and the associated Data collection Rules can be referred under below links: -

[Azure Monitor Agent overview - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview)

[Data collection rules in Azure Monitor - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview?tabs=portal)

# Automatic Deployment: -

## For Azure Servers: -

When Defender for Servers is enabled on Azure VMs, the Azure Monitor Agent (AMA) is automatically provisioned. There is no need for manual intervention to deploy the agent on Azure VMs.

## For On premises or ARC Enabled Servers: -

For on-premises or non-azure servers that are Azure Arc-enabled, you can automatically deploy the Azure Monitor Agent using the below azure policy:

Similar policy is available for Linux machines. Policy Name: - Configure Linux Arc-enabled machines to run Azure Monitor Agent

A screenshot of a computer

Description automatically generated

# Monitor Agent deployment and remediating missing agents: -

## Using Azure Policy: -

We can make use of Azure policy to Monitor and secure our Windows and Linux virtual machines, virtual machine scale sets, and Arc machines by deploying the Azure Monitor Agent extension and associating the machines with a specified Data Collection Rule.

Below are policy initiatives available and can be assigned to monitor the agent compliance and remediating/installing the agent on missing machines.

1. Configure Windows machines to run Azure Monitor Agent and associate them to a Data Collection Rule
2. Configure Linux machines to run Azure Monitor Agent and associate them to a Data Collection Rule

A screenshot of a computer

Description automatically generated

## Using Defender for cloud recommendations: -

Since we already have a policy initiative created that includes the policy to configure Azure Defender for servers, this policy ensures that the required monitoring agent is installed on the servers. We can ensure the Log Analytics agent, or the Azure Monitor Agent (AMA) is deployed using Azure Security Centre (Defender for Cloud) recommendations.

Go to Recommendations under Microsoft Defender for Cloud blade and search for log analytics and we will see below 2 Titles: -

1. Log Analytics agent should be installed on virtual machines: - This recommendation gives us the details of any VMs which are missing the agent.
2. Log Analytics agent should be installed on Windows-based Azure Arc-enabled machines: - This recommendation provides details of any ARC enabled VMs which are missing the AMA agent.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Manually Remediate missing agent deployment:

## For Azure VMs:-

There are multiple ways to manually install the Azure monitoring agent on Azure VMs. Please refer below link for instructions: -

[Manage Azure Monitor Agent - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-manage?tabs=azure-portal)

## For ARC enabled servers: -

From the Defender for Servers recommendation blade: -

Quick fix:  
Select the unhealthy resources and click “Fix” to launch “Quick fix” remediation. [Learn more >](https://learn.microsoft.com/azure/security-center/security-center-remediate-recommendations?WT.mc_id=Portal-Microsoft_Azure_Security#quick-fix-remediation)  
Note: After the process completes, it may take up to 24 hours until your resources move to the ‘healthy resources’ tab.

Manual remediation:

To install the monitoring agent on your Arc machine:  
1. From the Azure Arc machine's page, go to **Extensions** and select **Add**.  
2. Follow the instructions to add the relevant extension.  
You can also use ARM template or Azure Policies to manage the extension deployment to Arc servers. [Learn more about Log Analytics agent for Windows.](https://learn.microsoft.com/azure/virtual-machines/extensions/oms-windows?WT.mc_id=Portal-Microsoft_Azure_Security)

## Manual Deployment Using VM Guest baseline:

We can use VM Guest Baseline to manage auto manage the deployment of missing Azure Monitor Agent.

The plan is Auto manage to automatically deploys AMA, sets the Management Log analytics workspace as the endpoint for non-security event logs, onboards VM to defender for cloud, enrols into azure update management along with few other things.

Below is the confluence links which details on the list of components which we are looking to auto manage. (further information to be added).

[VM Guest Baseline - AV Cloud Platform - Confluence (atlassian.net)](https://ambvic.atlassian.net/wiki/spaces/ACP/pages/3093102607/VM+Guest+Baseline)

[Automanage for VMs - AV Cloud Platform - Confluence (atlassian.net)](https://ambvic.atlassian.net/wiki/spaces/ACP/pages/3094741009/Automanage+for+VMs)

[Enable Automanage for virtual machines through Azure Policy | Microsoft Learn](https://learn.microsoft.com/en-us/azure/automanage/virtual-machines-policy-enable)

# 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. There is no specific guidance for Defender for Cloud under the Performance Efficiency pillar of the Well Architected Framework. [↑](#footnote-ref-3)