Shape

Description automatically generated with low confidence

Colonial First State

RISE-DMT

Apr 2023

Document title

|  |  |
| --- | --- |
| **Project Title** | CFS Core IT |
| **Author** | Avanade:  Achroo Batta |
| **Reviewer** | <Insert> |
| **Approver** | <Insert> |
| **Current Version** | 1.0 |
| **File Name** | Rise-DMT |
| **Publication Date** |  |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes |
| 1.0 | 18/4/2023 | Achroo Batta | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 1](#_Toc132713732)

[1.1 Purpose 1](#_Toc132713733)

# Introduction

## Purpose

The purpose of this document is to provide proof of security controls followed while implementing DMT project.

\*Due to fortigate issues screenshots are taken from non-production. Production environment also uses same code base. Deployment happens through IAC, same security controls will be applicable.

**T01 - DMF SFTP Service/ T03 - External SFTP Server/T04 Third party**

Networking is only enabled for specific virtual networks and Ip addresses, which ensures safety.

Graphical user interface, text, application, email

Description automatically generated

Private endpoints are configured for secure communication.

Graphical user interface, text, application, email

Description automatically generated

Sftp access is secured through SSHKey parir and password

Graphical user interface, text, application

Description automatically generated

Sftp private endpoint is part of seperate SFTP subnet

Graphical user interface, application, table, Excel

Description automatically generated

NSG for subnet of Sftp

**Graphical user interface, table

Description automatically generated**

Route table is connecting to Azure Firewall

**A screenshot of a computer

Description automatically generated**

**T02 Migration Virtual Machine**

Separate Subnet Vmsub3 with nsg and route attached to it

Graphical user interface, text, application, email

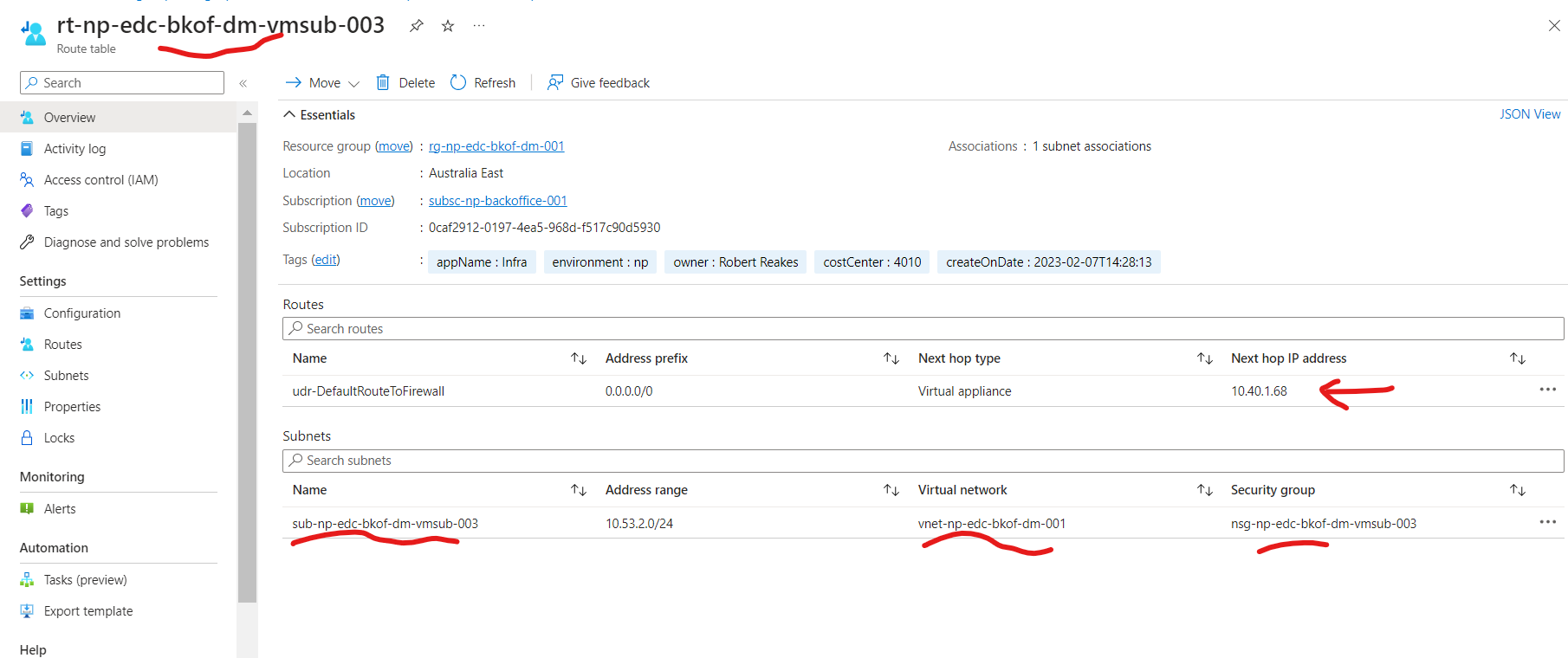
Description automatically generated

NSG – only allows specific access from specific networks and ports

Graphical user interface, table

Description automatically generated

Route Table to send all traffic to Azure Firewall 10.40.1.68



VM using Microsoft Standard Window 22 image

Graphical user interface, text, application, email

Description automatically generated

All CFS Standard extensions are installed

Graphical user interface, text, application, email

Description automatically generated

**T05 – KeyVault**

KeyVault is opened from specific virtual networks

Graphical user interface, text, application, email

Description automatically generated

Private endpoint is connected to keyvault for secure communication.

Graphical user interface, application

Description automatically generated

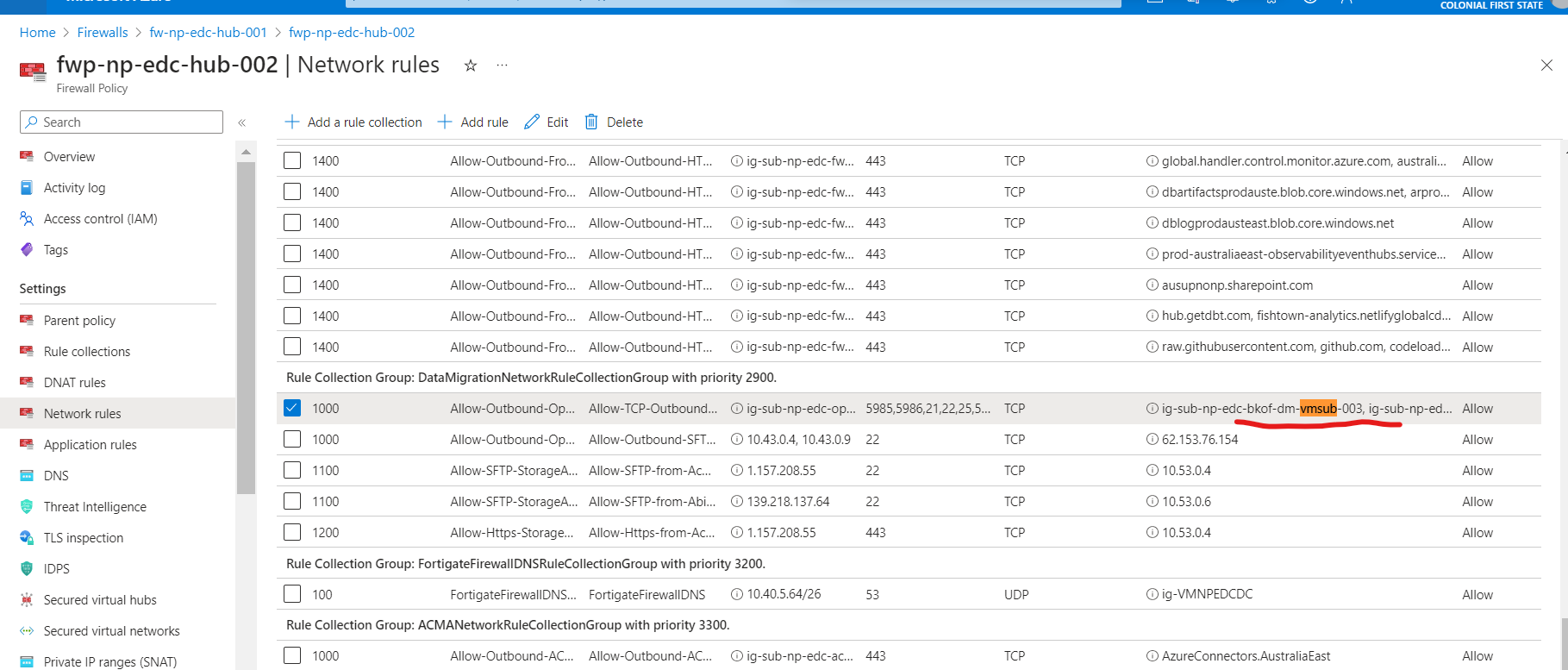
Only Azure RBAC based access can allow a person to read/manage secrets/passwords.

Graphical user interface, text, application, email

Description automatically generated

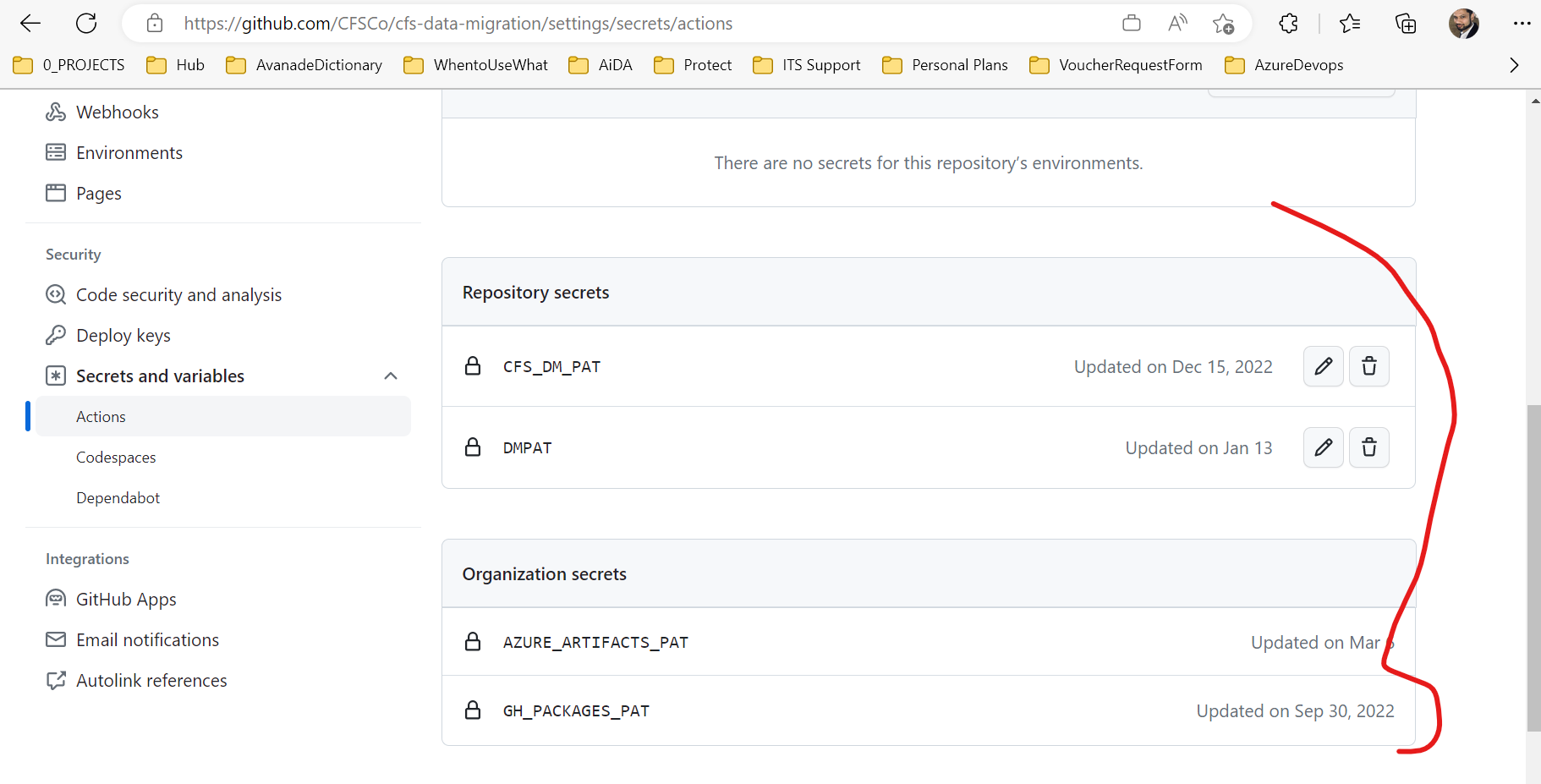
**T06 MLZ Network**

External / Internal Firewall



**T07 GitHub / DevOps**

**Github Secrets**



**Library**

Graphical user interface, application

Description automatically generated

**T08 Azure DataBox**

Handled by CFS and Microsoft Personnel.

**T09 Azure Data Lake Storage**

Datalake network enabled from virtual networks

Graphical user interface, text, application

Description automatically generated

Private endpoint enabled for datalake

Graphical user interface, text, application, email

Description automatically generated

**T10 - Azure Boards**

Security on DevOps is implemented through Azure AD

**Graphical user interface, text, application

Description automatically generated**

**T11 Migration VM SFTP**

Please refer CR document for malware assessment portion.

**T12 Manual Migration Virtual Machine**

Image hardening will be done by Qualys agent. These Virtual machines are temporary, so on completion of transfer. They will be deleted.