Author

Avd proposal as created by Reuben Cathan

Fantasia prbramil01

Proposed AVD solution

Contents

[Project Information 1](#_Toc202531108)

[Revision History 1](#_Toc202531109)

[Approvals 1](#_Toc202531110)

[Introduction 2](#_Toc202531111)

[Document Purpose 2](#_Toc202531112)

[Background 2](#_Toc202531113)

[Objectives 2](#_Toc202531114)

[Scope 2](#_Toc202531115)

[Staff & Locations 3](#_Toc202531116)

[Core IT Contacts 3](#_Toc202531117)

[High Level Overview 3](#_Toc202531118)

[Systems and Portals 3](#_Toc202531119)

[Personas 3](#_Toc202531120)

[Platforms (Cloud) 4](#_Toc202531121)

[Cloud Environments 4](#_Toc202531122)

[End-User Compute (EUC) 6](#_Toc202531123)

[EUC Devices 6](#_Toc202531124)

[AVD Overview 6](#_Toc202531125)

[EUC Equipment 6](#_Toc202531126)

[AD Security Groups 6](#_Toc202531127)

[RDS, VDI, & AVD 7](#_Toc202531128)

[IDAM 8](#_Toc202531129)

[Microsoft Authenticator Rules 8](#_Toc202531130)

[Appendix 8](#_Toc202531131)

[Network Diagrams 8](#_Toc202531132)

[Information Repositories 8](#_Toc202531133)

# Project Information

|  |  |
| --- | --- |
| **Section** | **Value** |
| **Project Code** | EX1AVD |
| **Project Name** | Milan |
| **Directorate Name** | AVDEX |
| **Business Sponsor** |  |
| **Solution Architect(s)** | - |
| **Program Lead** | Reuben Cathan |
| **Project Manager** | Reuben Cathan |
| **Document Status** | example |
| **Date and Version** | example |

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Summary of Changes** | **Changes made by:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Approvals

This document requires the following approvals. (As a minimum the Business Sponsor, Project Manager, ITLT Sponsor)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Method of Approval/Signature** | **Date of Issue** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

## Document Purpose

The purpose of this document is to provide approved, documented guidance as to what the desired future state is to be for the stated business entities and their IT landscape. This document also aims to provide key information on the current state of the IT landscape.

This document should be treated as a directive for the contained systems, services, functions - not a process or procedure. The absolute detail consisting of low-level configuration will be created as an output from the implementation of this solution design.

## Background

Fantasia corp are a fashion design house based in the UK, US, and Brazil. Fantasia Corp currently have their main HQ in London with two sister sites in the UK. There are 2 offices along with a warehouse in the US. Their offices are located in New York and Delaware, with a warehouse located in Ohio. As such a new office has been opened in Brazil and they are now looking to offshore some of their business area’s to this new location. Fantasia corp have no Internal IT department and have reached out to ourselves for our expertise and experience in designing and implementing AVD solutions, all network configurations are handled by their external IT support company and these tasks have been completed prior to engagement with ourselves.

Due to the sensitivity of their business the new office will operate in what is know as a clean room with dumb terminal clients these are HP T550 Intel terminals. These terminals are placed in the clean room and will allow access securely into a AVD environment hosted in Azure. This will server as a jump point to access systems that are specific for their job roles via the AVD.

Staff using the Thin clients from within Brazil will only be able to access the AVD solution from within the secure room and will not be able to login to any other systems. Face recognition will be used alongside MFA to stop unlawful entry to other systems.

A new requirement has been identified to help with onboarding Milan staff within the Fantasia Corp secure room. The staff will access systems similar to the European staff via a AVD solution hosted in the Brazil south Microsoft Azure Region.

It is currently estimated that there will be 12 FTE’s once fully implemented.

## Objectives

* + Facilitate staff access to their Fashion warehouse systems and database systems from within a Fantasia Corp AVD.
  + Details on how to access systems, the hardware provided, and software provided to aid users in their day to day functionality

## Scope

* Platforms (Cloud)
* End User Compute (EUC)
* IDAM

The following will be out of scope as Identified by Fantasia Corp

* Networking
* Telephony

# Staff & Locations

## Core IT Contacts

Below is a table showing the core IT contacts which who will need to be referenced throughout the course of this project. Some of these individuals will only be available during the integration, not post-integration:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Email Address** | **Phone Number** |
| Project Manager | Reuben cathan | [rcexample@example1.co.uk](mailto:rcexample@example1.co.uk) |  |
| Senior Systems Engineer | Reuben Cathan | [rcexample@example1.co.uk](mailto:rcexample@example1.co.uk) |  |
| Project Team Lead | Raul Gomes | [rcexample@example1.co.uk](mailto:rcexample@example1.co.uk) |  |

# High Level Overview

## Systems and Portals

As per the design workshop the following systems and portal access has been identified and listed below;

The portals will need to be accessible from within the AVD.

* Milandress
* Fashion101
* stfiles

The following software will be installed directly on the image used to deploy the AVD hosts for users;

* Microsoft office suite (word,excel,outlook etc)
* Addins for stfiles
* Fashion101 addins

## Personas

Persona’s to be created that grant access to systems and software installs via AD Group membership has been identified, these personals will help stream line the active directory access needed by staff. Therefore simplifying the administration task for IT to manage and keep a track of user group membership and access rights.

* Fantasia\_Adminstaff\_Persona
* Fantasia\_Designstaff\_Persona

# Platforms (Cloud)

## Cloud Environments

As detailed in the discovery meeting a new AVD solution will be created, currently Fantasia use 3rd party software to provision and manage AVD’s but lack the expertise in deploying and creating AVD infrastructure. As detailed in the discovery session a new AVD will be provisioned to help users securely access Fantasia systems.

**VNET’s and SNET’s:**

In the discovery workshop the following VNET’s and SNET’s have been Identified as created and assigned to use for this AVD deployment these are detailed below;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VNET Name** | **Address Spaces** | **SNET Name** | **SNET Address Space** | **Description** |
| Fant-bra-avd-milan01 | 10.150.7.129/28 | Fant-bra-avd-milan01-vd-snetbra01 | /28 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |  |
|  |  |  |
|  |  |  |  |  |
|  |  |  |

**Route Tables:**

There are currently no Route Tables configured for the following SNET’s below:

|  |  |  |  |
| --- | --- | --- | --- |
| **VNET Name** | **Route Tables** | **SNET** | **SNET Address Space** |
| Fant-bra-avd-milan01 |  | Fant-bra-avd-milan01-vd-snetbra01 | 10.150.7.129/28 |
|  |  |  |
|  |  |  |

**Peering’s:**

Peering’s will be needed to securely access the Warehousing systems in the UK and US these peering’s are listed below;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source VNET** | **Peering Name** | **Peer** | **Gateway Transit** | **Description** |
| Fant-bra-avd-milan01 | Braz-lon | Fant-lon-data01 | Disabled |  |
| Fant-bra-avd-milan01 | Braz-nyc | Fant-NYC-data01 | Disabled |  |
| Fant-bra-avd-milan01 | Braz-lon | Fant-lon-data02 | Disabled |  |
| Fant-bra-avd-milan01 | Braz-nyc | Fant-NYC-data02 | Disabled |  |

**Storge account:**

A storage account will be created as part of the deployment into Azure details are below

|  |  |  |  |
| --- | --- | --- | --- |
| **Storage account name** | **Kind of storage** | **Disk type** | **Storage replication** |
| FANTBRASA | Blob Storage v2 | Premium SSD | LRS |

No failover will be required as identified in the discovery workshop. The storage account will also be locked down to only allow access from the Fant-bra-avd-milan01 vnet.

**AVD Virtual Machine Host details:**

Fantasia will require 3 virtual machine hosts for the AVD deployment these will be built using the STANDARD\_D8AS\_V4 SKU from the Azure Gallery, with autoscaling set to burst beyond by 1 additional host. There will be no replication required to or virtual machine scale sets, these will be built in a single availability zone. These VMS will be part of a managed disk set and will be using persistent disks

The below table outlines the naming conventions and details of the vms to host the AVD solution.

|  |  |  |  |
| --- | --- | --- | --- |
| Vnet | Disk type | VM Name | Machine SKU |
| Fant-bra-avd-milan01 | SSD Premium 150 GB | FANT-BRA-AVD-VM01 | STANDARD\_D8AS\_V4 |
| Fant-bra-avd-milan01 | SSD Premium 150 GB | FANT-BRA-AVD-VM01 | STANDARD\_D8AS\_V4 |
| Fant-bra-avd-milan01 | SSD Premium 150 GB | FANT-BRA-AVD-VM01 | STANDARD\_D8AS\_V4 |

**NAT Gateways:**

A NAT Gateway will be required, this is to securely apply MFA rules and enforce security below are the details for the NAT Gateway:

|  |  |  |  |
| --- | --- | --- | --- |
| **VNET Name** | **NAT Gateway** | **Public IP** |  |
| Fant-bra-avd-milan01 | [Fant-bra-NGW01](https://portal.azure.com/#@DaviesGroup.onmicrosoft.com/resource/subscriptions/73db1ba4-5e24-46d7-a404-fd00848d0d69/resourceGroups/prd-avd-055IndiaOffshoreClaimsDNA-rg-01/providers/Microsoft.Network/natGateways/prd-avd-055IndiaoffshoreClaimsDNA-ngw) | 104.X.X.X |  |
|  |  |  |
|  |  |  |
|  |  |  |  |

# End-User Compute (EUC)

## EUC Devices

Fantasia will be utilising 12 HP T550 Intel terminals located in a secure office location. Users will be assigned access to a HP T550 Intel terminals with camera’s for windows ID recognition this is already implemented within the business. Other peripherals such as handsets keyboards and monitors will be granted to users on a case by case basis..

At the time of writing these were the numbers of thin client terminals which have been provisioned inside of the cleanroom and outside of the cleanroom.

|  |  |  |
| --- | --- | --- |
| **Item** | **Make/Model** | **Required Quantity** |
| HP T550 Intel terminals | HP T550 Intel terminals | 12 |
|  |  |  |
| **Totals:** | | **12** |

## AVD Overview

#### Fatasia Milan

1 new pool will be created using the 3rd party deployment software, these will be window 11 enterpise edition desktop images.

* + - “Standard” refers to standard issue Fantasia Corp group security tooling, core applications, and policies
    - The AVD will be deployed into the Fantasia Corp development tenant at the clients request for UAT testing after all testing is signed this will be moved to their production workspace.

As per Microsoft specifications a NAT gateway will be required for management of hosts as well as for MFA rule restrictions.

## EUC Equipment

#### Individuals

Currently all staff accessing the secured office will be allocated a workspace with the following hardware outlined below, mobile phones will be permitted into the office for MFA authentication using Micorsoft Authentication.

#### Hardware

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Make/Model** | **Standard Issue Quantity** | **Required Quantity** |
| Wired Headset | Standard issue as per Fantasia Corp standards | 1 | 12 |
| Mouse | Standard issue as per Fantasia Corp standards | 1 | 12 |
| Keyboard | Standard issue as per Fantasia Corp standards | 1 | 12 |
| Monitor | Standard issue as per Fantasia Corp standards | 1 | 12 |
|  |  |  |  |

## AD Security Groups

#### Persona Groups

Persona groups are to be created to allow for the ease of access rights to the AVD and other business area’s that are controlled by Active Directory Authentication.

Below are the proposed persona groups for Active Directory

* Fantasia\_Adminstaff\_Persona
* Fantasia\_Designstaff\_Persona

This is a requirement to keep track of all access granted to systems via group memberships in a centralized format.

## RDS, VDI, & AVD

#### Fantasia AVD Details

|  |  |
| --- | --- |
| Name | Parameter |
| Resource Group Name | Fant-bra-avd-milan\_RG01 |
| VNET Name | Fant-bra-avd-milan01 |
| Azure File shares SMB Share Name | \\ Fant-bra-avd-milan01  .file.core.windows.net\ Fant-bra-avd-milan01share |
| Log Analytics Workspace name | Fant-bra-avd-milan01wsp01 |
| App groups to be created (Azure not ADDS) | N/A |
| AD security groups for pool access (ADDS) | Fant-bra-avd-milan01-AVDUsers |
| Storage account FSlogix | FANTBRASA |
| Host Pool Description | Fantasia Brazil |
| Friendly Name | Fantasia Milan Brzil |
| Name for hosts | [f FANT-BRA-AVD-VM01](https://portal.azure.com/" \l "@612f5aff-57cb-4214-9fcb-d6e4665d890c/resource/subscriptions/73db1ba4-5e24-46d7-a404-fd00848d0d69/resourceGroups/PRD-AVD-055INDIAOFFSHORECLAIMSDNA-RG-01/providers/Microsoft.Compute/virtualMachines/dguksavd0550b2" \t "_blank) – VM04 |
| Sizing standard (see KB0013435 AVD Host Pool Sizing Guide) | Small/Small |
| VM SKU | D8s\_v5 (8C & 32GB) |
| Network Size | /28 |
| Security Script | Sophos deployment script |
| Tags | Department: Millan  Owner: Oliveria Gomes  Environment: Dev  Criticality: Tier 3  Application: AVD |
| NAT Gateway | [Fant-bra-NGW01](https://portal.azure.com/#@DaviesGroup.onmicrosoft.com/resource/subscriptions/73db1ba4-5e24-46d7-a404-fd00848d0d69/resourceGroups/prd-avd-055IndiaOffshoreClaimsDNA-rg-01/providers/Microsoft.Network/natGateways/prd-avd-055IndiaoffshoreClaimsDNA-ngw) |

# IDAM

## Microsoft Authenticator Rules

Authenticator rules will be in place to allow only traffic from the Nat Gateway to be allowed in both directions, these rules will be assigned to the NAT gateway. Geo location will be in place to allow authenticated users to be able to access resources from the secure office

# Appendix

## Network Diagrams

|  |  |
| --- | --- |
| **Diagram** | **URL** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Information Repositories

|  |  |  |
| --- | --- | --- |
| **Name** | **Stage** | **URL** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |