Thiago Farias

Proposal Deployment Plan

Promised Land Server

Hukilau Marketplace

# Overview

A sign with palm trees in the background

Description automatically generated with low confidenceIt’s time to bring together everything you have learned in your lab simulations and projects. The final project assesses how well you have learned the material that has been taught including the hands-on projects throughout the semester. The final project will include ambiguity. Ambiguity is defined as inexactness or vagueness; being open to multiple interpretations.

**Scenario - Full Office Deployment Proposal for PromisedLand at Hukilau Marketplace**Map

Description automatically generated

PromisedLand.com has made the decision to open new office space at the [Hukilau Marketplace](https://hukilaumarketplace.com/shop/) located at 55-370 Kamehameha Hwy, Laie, HI. 96762. The new space will occupy 7,000 square feet and 45 employees. The space will serve as a [hybrid call center](https://www.trickyenough.com/hybrid-call-center/) that includes several tourist guide stations providing assistance, information on cultural, historical, and contemporary heritage to people looking for guided sightseeing tours.

Please refer to the organizational chart below as a way to help you in your full deployment implementation.

# Server Architecture And Baseline

The implementation will be hosted using Microsoft Azure.

The Server will be x64 architecture and will implementing the [Microsoft Security Baseline](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines?WT.mc_id=modinfra-11348-socuff) “Security Compliance Toolkit (SCT)”, which can be downloaded from [Security Compliance Toolkit (SCT)](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10).

* Windows 10 security baselines
  + Windows 10 Version 1909 (November 2019 Update)
* Windows Server security baselines
  + Windows Server 2019
* Microsoft Office security baseline
  + Office 365
* Microsoft Edge security baseline
  + Edge Browser Version 93

# Storage Capacity

The Windows servers and workstation will be Virtual Machines and will be initiated with 8Gb extra drive and (BS2 Standard Series 127 GiB of disk size). In case of necessity, it can be upgraded or downgrade by administration request.

# Hardware and Software Troubleshooting

For troubleshooting follow the checklist below:

* PC or Server is powered on
* Network Cable connected
* Network connected
* Internet connected
* Domain Controller
* Active Directory
* Check for Updates and software patches
* Restart the computer

# Server Backup and Restore

The backup will be performed using the [Azure Server Backup Feature](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal). The virtual machines will have full backup on cloud, which will be executed daily. The backup will supply the [VM replication](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replication).

# Encrypted File System

The server and workstation will use [Bitlocker](https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server) in the future following the Microsoft standard guide. However, for now the share file will use EFS to protect all organization files over file sharing system.

# Security Protection

The implementation will follow [Microsoft Information Security and Risk Management (ISRM)](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory). And The servers will use windows firewall for extra protection.

All workstation are going to use Antivirus/antimalware.

Enable passwords management to security polices to make strong passwords.

User Folder Redirection for store user documents folder in the server files system.

Azure Virtual Network will be accessed by [point-to-site VPN](https://docs.microsoft.com/en-us/azure/vpn-gateway/design?toc=/azure/virtual-network/toc.json#P2S) using private IP Address.

Diagram

Description automatically generated

Figure 1 - VPN point-to-site

Ports to control on the firewall/network security group inbound rules:

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Protocol | Service | Status |
| 80 | tcp | http | Open |
| 1433 | tcp | Database | Open |
| 443 | https | https | Open |
| 3389 | tcp | RDP | Open |

Server Security Group

Graphical user interface, text, application, email

Description automatically generated

Client Security Group

Graphical user interface, text, application, email

Description automatically generated

# Server Hardening

Windows Virtual Machines using Microsoft Azure

B2S Standard tier

Core 2, RAM 4Gib, Temporary storage 8Gib

* Server 1 - Windows Server 2019 – B2S Standard tier  
  2 CPU  
  4Gib Memory  
  IP: 192.168.0.4

8Gib Temp SSD

* DB Server - Azure Database  
  32Gib Memory  
  IP: 192.168.0.5  
  SQL Server Connection: jdbc:sqlserver://192.168.0.4:1433;database=pl-database;user=thiago@pl-database-server;password={your\_password\_here};encrypt=true;trustServerCertificate=false;hostNameInCertificate=\*.database.windows.net;loginTimeout=30;
* Workstation[N] – Windows 10 – B2S Standard tier  
  2 CPU  
  4Gib Memory

8Gib Temp SSD  
DNS IP: 192.168.0.4

[Network Configuration](https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip)

Diagram

Description automatically generated

Figure - NAT and VM with instance-level Public IP

vnet 192.168.0.0/23

Graphical user interface, text, application, email

Description automatically generated

server subnet 192.168.0.0/24

workstation subnet 192.168.1.0/24

Graphical user interface, text, application, email

Description automatically generated

# User and Groups for Active Directory

User names will be creates according to the image bellow. The name standards will follow first name and fist letter of last name. In case of duplicates number will be added to the and, e.g. 1,2,3…

The groups will be organized following:

* Executive
  + CEO
  + CRO
  + VP
  + CFO
  + CMO
* Manager
  + Directors
  + Managers
  + Leads
* Develop
* Sale
* Support
* QA
* Application
* Hardware
* Finance
* Office
* Marketing
* Designer
* PMO

Timeline

Description automatically generated

# Principle of Least Privilege

[Implementing Least-Privilege Administrative Models](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models) will grant access to the users and organization through Active Directory and some follow guidance will be implemented as well:

* Secure Password and expiration policy
* Delete Inactive Accounts
* Only admins will have access to Servers and Azure
* Using groups to define privileges
* Assigning user working hours

# Disaster Recovery

The virtual machines will use [Microsoft Azure Site Recovery for replication](https://docs.microsoft.com/en-us/azure/site-recovery/) to replicate the machines in a different location such as West or Central US depending on the BS1 tier availability.

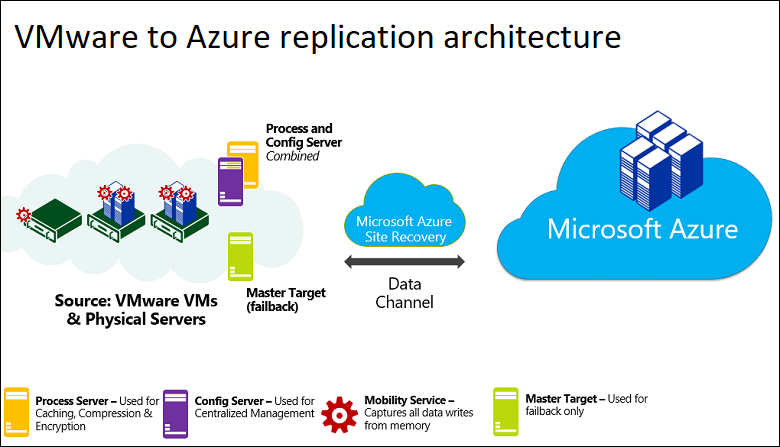


Figure - Azure disaster recovery architecture

Diagram, application

Description automatically generated with medium confidence

# Implementation

The video below shows the implementation of plan above in details, exploring the system configuration and the features installed.

## Infrastructure

<https://youtu.be/U7nKFBDR18M>

## Configuration

<https://youtu.be/OP_27_jlFjE>

Resources

<https://docs.microsoft.com/en-us/windows/resources/>

<https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines>

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>