Final Report

Ozmart Retail Group Cloud Migration

Unit: COIT20265

Student 1: Simarpreet Kaur (12226696)

Student 2: Navdeep Saini (12207773)

Student 3: Anupa Bodhimaluwa (12216471)

Student 4: Mohmed amaan patel (12204426)

Project Mentor: Biplob Ray

Date: 06/10/2024

CQUniversity Australia

# Introduction

Ozmart is a Small-to-Medium Sized retail organisation which is growing at a significant rate. Due to its expansion the current on-premises networking infrastructure is unable to handle increasing demand and network traffic. Due to this the stakeholder and IT team have device to migrate the on-premises infrastructure to cloud to improve the scalability, availability, security of the networking infrastructure and enhance digital communication between different branches. Below are the major technical limitations that are hinderance to Ozmart infrastructure:

**Scalability**: Current on-premises network consists of legacy cisco switches, routers and firewall that are unable to accommodate organisations growth and causing bottleneck. The legacy switch port and firewall port have limited bandwidth (in megabyte) and single point of failure that is the main cause of bottleneck.

**E-LAN connectivity**: Ethernet Local area Network connectivity between different branches (Sydney and Adelaide) using MPLS connection (technique used by telecommunication network that transfer data from one node to another based on short path). Due to MPLS connection the branches are unable to handle increase traffic.

**Resource Constrains**: Internal IT team is facing issues while allocating resources. Due to the legacy system the team must carefully consider the requirement and compatibility before deploying new hardware. This task is time consuming and can be mitigated after moving to cloud as resources are available on demand in cloud.

**HA and Redundancy in Network:** Current networking infrastructure doesn’t have redundancy and High availability in case a hardware goes down. There are no proper power backups, failover for switches, routers or Firewall. There is not Disaster recover site setup for the server.

**Security**: Currently, Ozmart is only relying on CISCO firewall for all the security. There are no Endpoint protection software’s or log monitoring systems setup. Due to this there is limited visibility to the network traffic and hardware firewalls are hard to scale as the network traffic increases. There is no proper end to end encryption setup.

**Aim of the Project:** The main goal of this project is to move the company’s on-premises IT working environment to Microsoft Azure, a cloud computing system to improve on their working flexibility, capacity and effectiveness. To provide a stronger follow for the business, to become less reliant on physical servers.

**Problem to solve:** On-premises infrastructure presented a number of difficulties prior to the move. There were existing systems that applied for accommodating the growing business, which experienced performance slowdowns especially during sales high-traffic. Moreover, keeping the physical servers implied some substantial difficulties – these were updates and the need in staff to control the servers, all of which escalated the costs of the organization’s operation. Thirdly, the level of security to connect three sites in Melbourne and Sydney and Adelaide were a challenge necessitating proper infrastructure, thus the current infrastructure posed insecurity issues as well as inefficiency. These problems showed that Ozmart required a more loose and capable arrangement to support its further development and requirements.

**Scope of the Project:** The scope of the migration of significant services and networks from internally installed systems to Microsoft Azure services. It involves setting up resource group, V-nets, Virtual Machines, firewalls, encryption & access control in addition to other measures towards ensuring safety of the data & to adherence to the laid down best practices. Furthermore, the scope was defined also to enhance the capability of the networks as well as improve and make it efficient to support the interaction between the three sites and future development of the network protocols.

The systems created, the technical artefacts produced, and the team members' contributions are all thoroughly summarised in this report. In order to provide optimal performance for the cloud-based environment, the project scope included setting up virtual networks and securing communication between the three sites.

Ozmart consist of two Site one is the head office (HQ) which is in Melbourne and a branch office in Sydney. Since Melbourne is the main Site, it has all the server hosted on VMware environment. Company is utilising Cisco networking products such as firewall, routers, switches and wireless access points. As the organisation is expanding the on-premises network is unable to hold the required bandwidth. The ports on switches and firewalls are megabyte and can’t hold the traffic. This document outlines the current on-premises infrastructure of Ozmart.

The whole on-premises network can be divided into 3 components: DMZ, internal and External network.

A diagram of a computer network

Description automatically generated

**VLAN’s: Virtual Local Area Network**

VLan’s are used to create a logical partition between network so that devices in same VLAN can communicate with each other and policies can be implemented between to separate the traffic and increase the security.

In our network we have use 3 VLAN namely **Internal VLAN, External VLAN and DMZ VLAN.**

**Internal VLAN:** This VLAN is used by the employees for internal communication among employees and to reach to the server. It includes laptops, desktops, computer and other networking devices. It also includes the server that doesn’t require external access.

**External VLAN:** This is where the internet comes from. The resources that need direct internet access are connected to this VLAN. The devices connected to this are firewall and router.

**DMZ**: De-militarized zone is mainly for external facing servers. This includes public facing server such as companies’ websites. In our on-premises network its connected to a switch and then connected to a firewall.

**Switches**: The on-premise consist of 3 managed switches. Switches can operate in layer 2 and layer 3. Layer 3 switches have the capability to route the traffic. However, in the current setup we have got layer 2 switches. There are 3 different type of switches Core layer switch, Distribution layer switch and access later switch. Core layer switch act as a backbone and connects to distribution layer. In our network we are using Access layer switch acts as a connection between firewall and end devices such as server, laptops, desktop and Wireless access points.

**Routers**: Routers are the intermediate devices used in the layer 3 of the network and particularly used to connect LAN or WAN. They interconnect the packets between the networks. They assist in the direction of the packets to the correct place by referring to routing table. They also assist in traffic control; NAT support and its primary task includes dynamic routing. They also help with traffic management, network address translation and provide dynamic routing protocols. Routers used in our network are configured with OSFP protocol which is used for routing IP packet within Autonomous system. It routes packets using network tropology map.

**Firewall:** Firewalls are security devices that are used to protect the network from threat and unknow access. Using firewall, we can apply traffic control to the network and decide what port can be open and what ports need to be closed. Firewall are used for Intrusion prevention, VPN access and application layer filtering.

In our on-premises network we have implemented firewall to provide control over the traffic by using access control list which define the rules and policies to permit or deny the traffic based on the requirements. Firewall provides logging and monitoring service where a network engineer can see what kind of traffic is flowing and block it if needed.

**End user Devices**: There are multiple end user’s devices that used are being used by Ozmart. Laptop, desktop, WAP, Printers. Wireless devices such as laptops and mobiles are connected.

# System Overview

The cloud system is designed primarily to create a scalable, robust and secure networking infrastructure. After carefully considering different cloud service provider and writing pros and cons of top 3 cloud service providers we have decided to use Azure for this migration as its robust, efficient and secure and is compatible with current applications. This designed system looks after complete security, high bandwidth or throughput and emphasises on security and consist of tailored firewall policies. The system is designed considering the future growth of Ozmart as an organisation.

A diagram of a cloud computing system

Description automatically generated

Fig: Azure Network Design

**System architecture overview**

**Resource group:** These are the containers that holds different application/organisation resources. In this architecture we have 2 Resource groups.

- Ozmart-Australia

This designed resource group is used for hosting critical services that are crucial to the business. Main components of this resource groups are Servers, Vnet’s, VM’s and firewall.

- NetworkWatcherRG

This resource group is for the users in Sydney branch and mainly host virtual machines, laptops and management devices. Main components of this resource groups are Vnet’s, VM’s and management devices like laptops and desktops.

**Virtual Network**

Virtual Networks are used for network isolation when resources in same virtual network can communicate with each other without any policies. In our cloud system we have got 3 Vnet’s:

**Ozmart-Mel-Vnet**

- **Purpose:** This Vnet host production server including web server.

- **CIDR Block:** 10.10.0.192/24

- **Subnets:**

* **Azure firewall subnet** 10.10.0.192/26
* **Laptop subnet:** 10.10.0.128/26
* **Management subnet**: 10.10.0.64/26
* **Server subnet:** 10.10.0.0/26

• **Ozmart-syd-subnet**

**Purpose:** This subnet is used for hosting virtual machine for end user devices.

**CDIR Block:** 10.20.0.0/16

**Subnets:**

* **Laptop subnet:** 10.20.0.0/26
* **Desktop subnet:** 10.20.0.64/26
* **Guest subnet:** 10.20.0.128/26
* **Gateway Subnet:** 10.20.0.192/27

**Ozmart-adl-vnet**

**Purpose:** This Vnet is used for hosting virtual machines in Adelaide site for end users.

**CIDR :** 192.168.0.0/24

**Subnets:**

* **ManagementSubnet**: 192.168.0.64/26
* **LaptopSubnet**: 192.168.0.128/26
* **GateWaySubenet:**192.168.0.192/26

**VnetPeering**

Vnet peering helps in establishing communication between different Vnet’s using private IP address. In this architecture peering is setup as shown below:

**Ozmart-Mel-Vnet peered with Ozmart-Syd-Vnet and vice versa**

This peering enables communication between Melbourne and Sydney Vnets. Devices in Sydney can communicate with web server hosted in Melbourne.

**Ozmart-Mel-Vnet Peered with Ozmrt-Adl-Vnet and vice versa**

This peering helps in communication between Adelaide and HQ in Melbourne

**Ozmart-Syd-Vnet perred with Ozmart-Adl-vnet and vice versa**

This peering helps in establishing communication between Sydney and Adelaide sites.

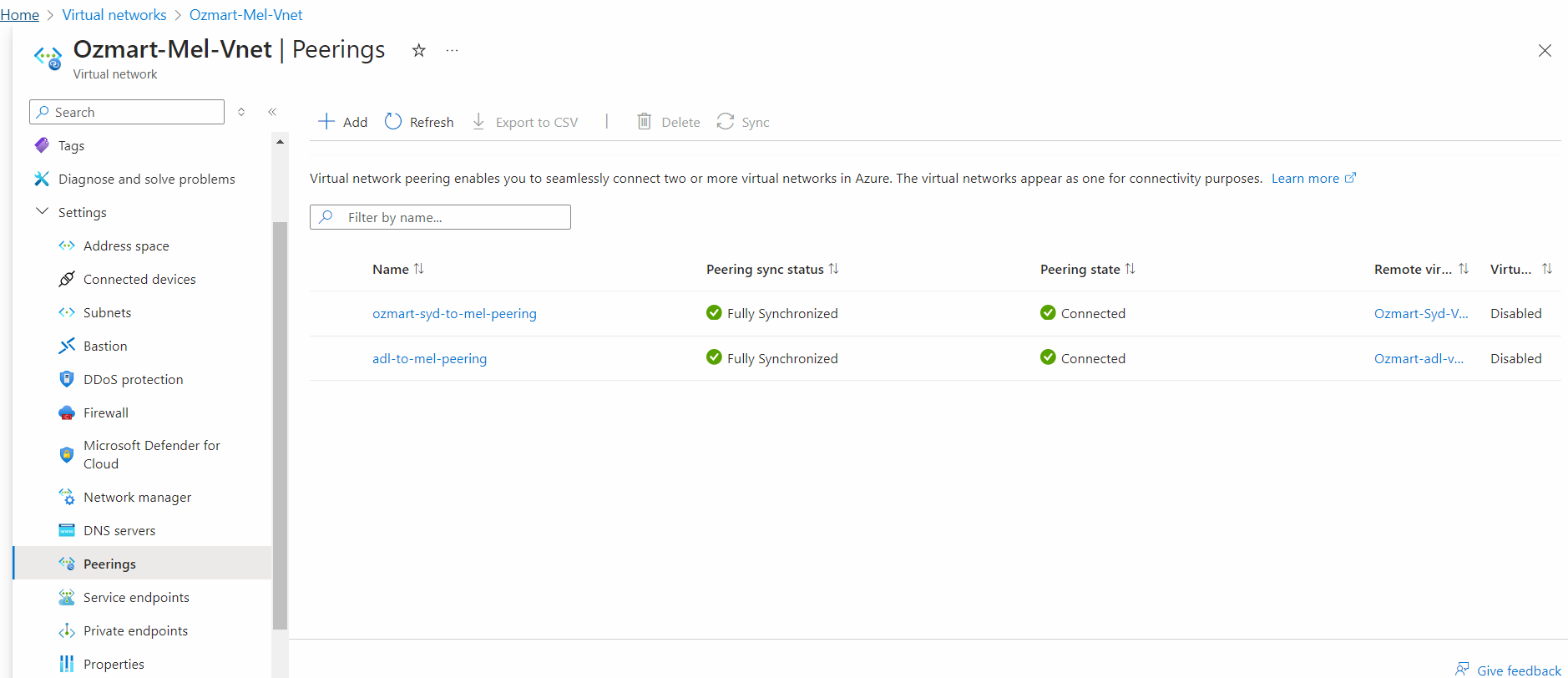


Fig: Vnet Peering

**AZURE FIREWALL**

Firewall is the central component of our cloud architecture ensuring the communication between Vnet’s is secured and controlled from outside and inside of azure network. Firewalls provide wide Varity of features that helps in effective management of the network. Traffic management filters inbound and outbound traffic based on the polices applied. Logging and monitoring provide traffic pattern and graphs for visualization. We can further apply application rules for managing application traffic.

**FIREWALL POLICY**

The following firewall policies are configured to enhance the security and control over the network.

**RDP POLICY**

**Purpose:** These policies are configured to allow remote access the VM’s and Servers. Not all the devices in our network have public IP address. We have applied firewall rules to open specific ports to allow RDP traffic to VM’s.

**Web Server Access Policy**

**Purpose:** This limits the inbound and out bound rules that protects unauthorized access to the server and prevent against DDos.

**Security Overview**

**Network Security Group:** NSG adds and extra layer of security to the subnets. In our environment we have got NSG for Servers and VM’s. These helps in isolating the traffic to virtual machines and server further enhancing the security.

Anupa-VM-nsg,Navneet-VM-nsg are vm specific NSG group and om-webserver01-nsg and Server-nsg are server specific NSG group.

A screenshot of a computer

Description automatically generated

Fig: NSG

**Azure Policies:** These helps in implementing a standard across the organization. They can play crucial role in access management and ensures consistent security postures.

We have implemented 2 azure policies in our organization network; Enable audit category group resources logging and policy to audit public network access.

A screenshot of a computer

Description automatically generated

Fig: Azure Policies

**Azure Monitor:** We have implemented the use of azure monitor for monitoring the resource health, security and performance of the network including bandwidth, and if a device is low on resources. Using this we have setup alerts.

A group of people with text

Description automatically generated with medium confidence

Fig: Showing Azure Alerts

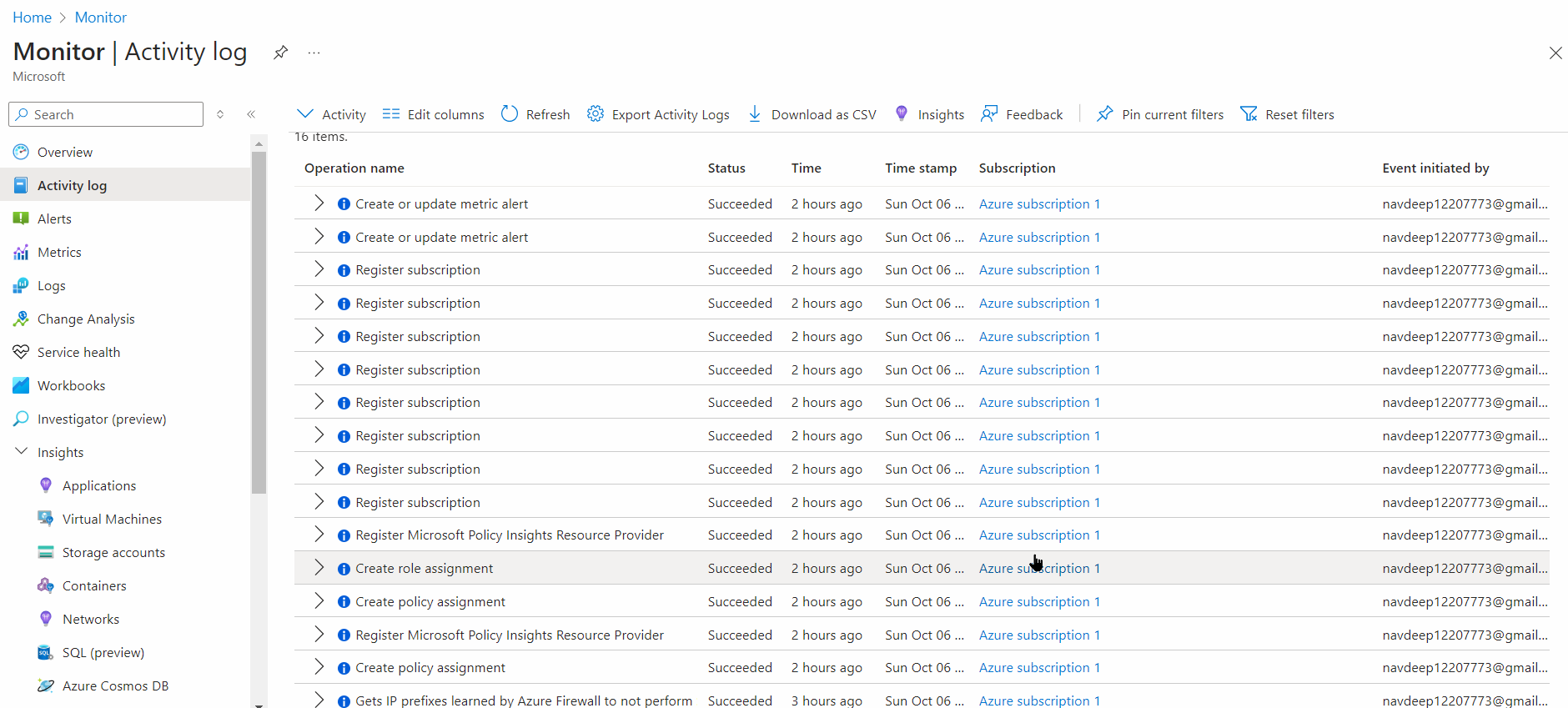


Fig: Azure Monitor Showing Activity logs

**COST MANAGEMENT**

Effective strategies have been implemented to monitor and reduce the cost and optimize the resources. Below are the tools used for Effective cost management:

**Azure Cost management centre:** This tool helps us monitor the cost of each resource deployed and using this we can add or remove resources based on the requirement.

A screenshot of a graph

Description automatically generated

Fig: Cost

**Re–sizing resources:** Regular monitoring of Azure cost management and monitor tool which can provide us with data of what resource is costing us more. Using this we can limit resource of the CPU or memory if not being used.

**Azure Sentinel:** Azure Sentinel proves highly valuable and effective in maintain cloud security to provide enhanced threat protection, control over responses to threats, as well as integrated case management. It is a cloud SIEM engine and cloud-based Soar solution that makes security operation in cloud infrastructure possible for organizations. Azure Sentinel integrates data from cloud services as well as system environments and third-party security solutions, to give a single perspective of potential threats. It uses artificial intelligence (AI) and machine learning techniques to identify the defects and deviations of the behavioural activity, therefore is capable of identifying threats before they assume a dangerous form.

A screenshot of a computer

Description automatically generated

**Backup:** Azure Backup is a crucial component in strengthening cloud security solutions because it is a secure, elastic, and affordable solution for securing data in the cloud. It safeguards important data belonging to the business organization from activities such as deletion by mistakes, ransomware, and data damage. Azure Backup allows organizations to recover data in the event of a breach/ failure because it automatically backs up files, virtual machines, databases and applications. The service allows customizing the backup policies and retention, thus it is possible to define both the frequency of backup, as well as the time for which the data is stored to meet compliance and governance goals.

A screenshot of a computer

Description automatically generated

Fig: VM Backup

# Delivered Technical Artefacts

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **File** | **Description** | **PDF?** |
| Problem Statement | Group08-Problem-Statement.docx | Detailed description of current networking issues. provides a thorough examination of Ozmart's networking problems and explains why moving from on-premises to the cloud is necessary. | Yes |
| Risk Assessment Report | Group08-Risk Assessment-Report.docx | Summarises the process of risk assessment that was done during the move, pointing out operational risks, system vulnerabilities, and possible security concerns. It also includes the assumptions made during the assessment. | Yes |
| Risk Assessment Table | Group08-Risk-Assessment-Table.xlsx | A thorough table that lists every risk that has been detected, together with the security measures that are linked to it and the steps taken to reduce it. | Yes |
| Azure Setup Instructions | Group08-Azure-Setup-Instructionds.docx | A step-by-step guide for setting up virtual machines, virtual networks, firewalls, and load balancers in Azure's network components. These guidelines guarantee the correct configuration of the cloud environment. | Yes |
| On-Premises Setup Instruction | Group08-On-premises-Setup-Instruction.docx | Complete setup guidelines for the on-premises architecture, encompassing internal networking, and server configuration | Yes |
| Azure Network Design | Group08-Azure-Network-Design.docx | Architecture of the Azure network, including items like security groups, subnets, VPNs, and virtual networks (VNETs). It contains illustrations showing how various network elements interact and are protected within the Azure cloud. | Yes |
| NIST Framework Implementation | Group08-NIST-Framework-Implemention.docx | Explains how security standard compliance was ensured during the cloud migration process by implementing the NIST Cybersecurity Framework. | Yes |
| Review Existing Cloud Products | Group08-Review-Existing-Cloud-Products.docx | A thorough analysis contrasting the features, costs, scalability, and security of the several cloud systems on the market. This document was a contributing factor in Ozmart choice to select Azure as their preferred cloud platform. | Yes |
| Migration Strategy | Group08-Migration-Strategy.docx | A thorough plan of action detailing the stages and procedures needed to move Ozmart infrastructure from its on-premises location to the Azure cloud. Timelines, technical specifications, and dependencies are all included for a seamless transfer procedure. | Yes |
| On-Premises Packet Tracer | Group08-On-Premises.pkt | A simulation file for Packet Tracer that is used to simulate the on-site network. Prior to the actual migration to Azure, this simulation enables the testing and visualisation of network components, including switches, firewalls, and routers. | Yes |
| EntraID Setup | Group08-EntraID-Setup.docx | The procedures for setting up Microsoft Entra ID (Azure Active Directory) for Ozmart cloud infrastructure are described in this paper. It contains directions on how to manage cloud resource access, set up user authentication, and put role-based access control (RBAC) into practice. | Yes |

# Contributions

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** | **Percent** | **Summary of Contributions** | **Technical Lead on Artefacts** |
| **Mohmed Amaan Patel** | 25% | As for the method of controlling, organizing, and coordinating a project, Amaan has definite experience in project management; a task was assigned to him to organize a team, and he was able to accomplish it as well as exercise proper control over the project. Some of the ways that he ensured that the team delivered are the following: deadlines, roles and meetings. Besides, attempting to have his own understanding of the timelines for the project, Amaan ensured the people of interest endorsed the goals of the project by engaging them in a conversation. However, it is crucial as we can see it is logical that the team would benefit from understanding how to prevent risks and deal with challenges such as a delay or technological problems. | * Risk Assessment * Risk Assessment Table * Testing and Validation * Problem Statement * Migration Strategy |
| **Navdeep Saini** | 25% | Demanding the position of a network engineer, Navdeep contributed by providing recommendations to transport the networks from an enterprise’s local facility to the cloud. In addition, he compares the present condition of the network and the parts and configurations. In order to communicate with each other over the numerous cloud services and was concerning about IP addressing and subnet masking while constructing the Cloud Network Architecture. He was able to assess the architecture for concern and specifically with the Cisco Packet Tracer to determine the problem areas. He adapted the features after the migration test of the performance, security, and connectivity of the network. | * On- Premises Network Architecture. * Azure Network Architecture. * IP Addressing and Subnetting. * Routing Protocol. * Testing and Validation * Azure Migration. * Monitoring and troubleshooting with cloud tools. |
| **Simarpreet Kaur** | 25% | Simarpreet was overall in charge of the administrative security of the transferred environment. She did therefore a splendid job in explaining how security groups, encryption and firewall configuration should be provided correctly. They also helped to ensure that we would have no more threats to the network and cloud environment. However, because she was overly worried about the project security, she was able to ensure that the organization’s data was safe during the migration exercise hence avoiding some of the cyber dangers to some of the migration processes. | * NIST Security Framework * Firewall configuration * Azure Network Security * Azure Migration |
| **Anupa Bodhimaluwa** | 25% | Anupa did the work on implementing resources like VMs and storage, AS well as contributed to the design of the general cloud. However, occasionally, there was no hustle and bustle at work, for instance, during the resource organisation stage in Azure, and sometimes a certain technical difficulty might demand help from other team members of the team. He has really done his best, but it could have had a greater result if he had submitted them early enough. | * Azure Setup * IP Addressing and Subnetting. * Azure Network Design * Review of Existing Cloud Products * Azure Migration |
|  |  |  |  |

# Next Steps

After completing the migrate of Ozmart’s infrastructure to Azure, we propose that Ozmart, implement the following steps to improve, protect, and optimize the Azure environment. These steps will not only keep the system on optimum efficiency in all these factors but will also pave way for system scale up as well as improvement of system security.

1. **Business Continuity and Disaster Recovery Plans:** Backup and fail over are provided on Azure by default, however they are not very effective, so it is recommended to develop backup and fail over strategies, which would be constant procedures with geo-replication of important systems.

* **Action:** Action: Disaster recovery utilizing Azure Site recovery and GEO-redundant storage for high impact apps and data.
* **Benefits:** Allows Ozmart operations to quickly resume work in the event of interruptions in its work, and minimizes the potential losses and, accordingly, the damage. Methodology, Risk, and Test items Information’s While Azure provides some fundamental DRDR (Disaster recovery) features, constructing a sequential business continuity agenda with backup, failover, geo-redundancy on applicable models is much more advisable.

1. **Complete Testing of Performance and Scalability:** Although this migration was achieved, it is recommended that other load tests be conducted This type of test that should be conducted is known as the load test since it provides approximations of how the system performs at most density or even during the campaigns that are significant to the business organization. This testing will help to identify the problem towards the provision of resource and manage the traffic productive loads towards the infrastructure without affecting the user adversely and service unavailability.

* **Action:** A simple load test should be conducted as well as actual performance evaluation test.
* **Benefits:** Ensures that other elements of cloud-based system can strenuously adopt auto scalability and accommodate traffic spurts that the infrastructure may sometimes encounter.

1. **Implement Advance Security Features**: Although the earliest waves of cloud migration encompassed fundamental security components such as Virtual Private Networks VPNs, firewall, and encryption, there are enhanced security measures to consider securing the environment.

* **Multi-Factor Authentication (MFA):** MFA for all users that minimize the number of users accessing the system through unmalted devices or form unauthorized sources.

1. **Hybrid Cloud Strategy:** If at all Ozmart wants to continue to use some exclusive systems or hardware, it might be more advantaged for a cloud hybrid setting. Azure is fully equipped with hybrid features that make it easy to connect the on-premises infrastructure with cloud.

* **Action:** Take advantage of Azure Arc for single-source cloud and on-premises infrastructure management.
* **Benefits:** It allows Ozmart to enjoy the various opportunities of cloud computing partly while still maintaining full control over some of the on-premises systems to manage.