

# Final Report

## Ozsmart 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

### 1 Introduction

Ozsmart 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 Ozsmart 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.

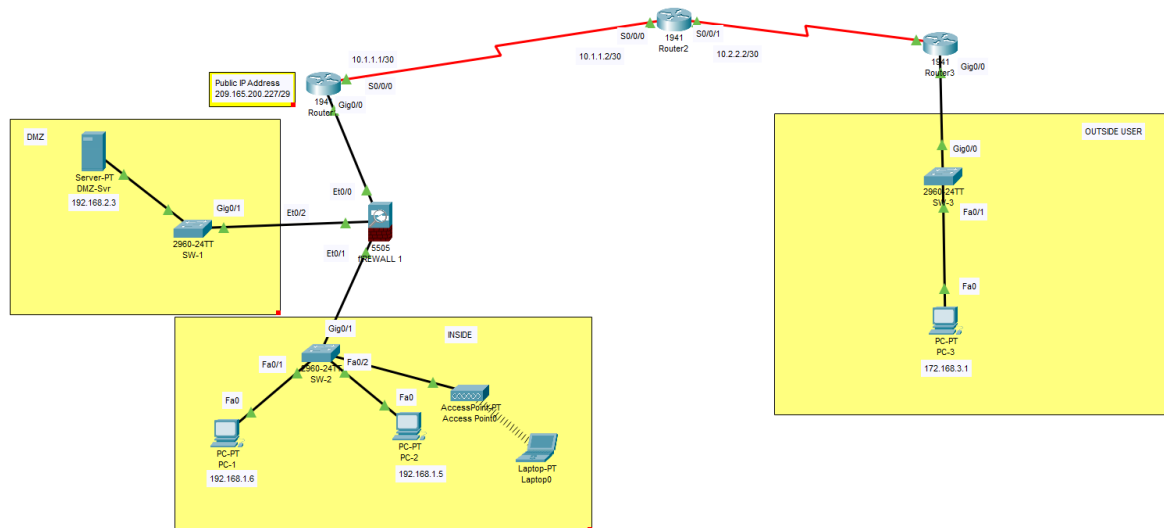
**Problem to solve:** On-premises infrastructure presented a number of difficulties prior to the move. There were existing systems that applied for accommodating the growing business, which experienced performance slowdowns especially during sales high-traffic. Moreover, keeping the physical servers 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.



## 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 OSPF protocol which is used for routing IP packet within Autonomous system. It routes packets using network topology 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.

## 2 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.

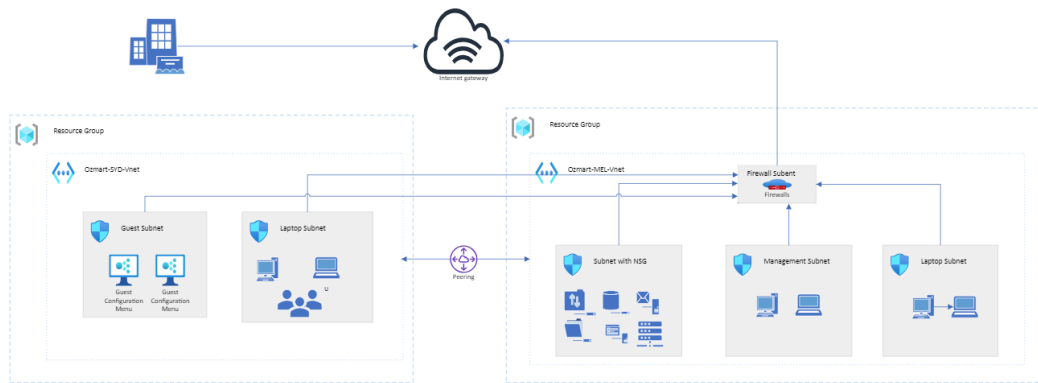


Fig: Azure Network Design

## 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.

**CIDR 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 Ozmr-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.

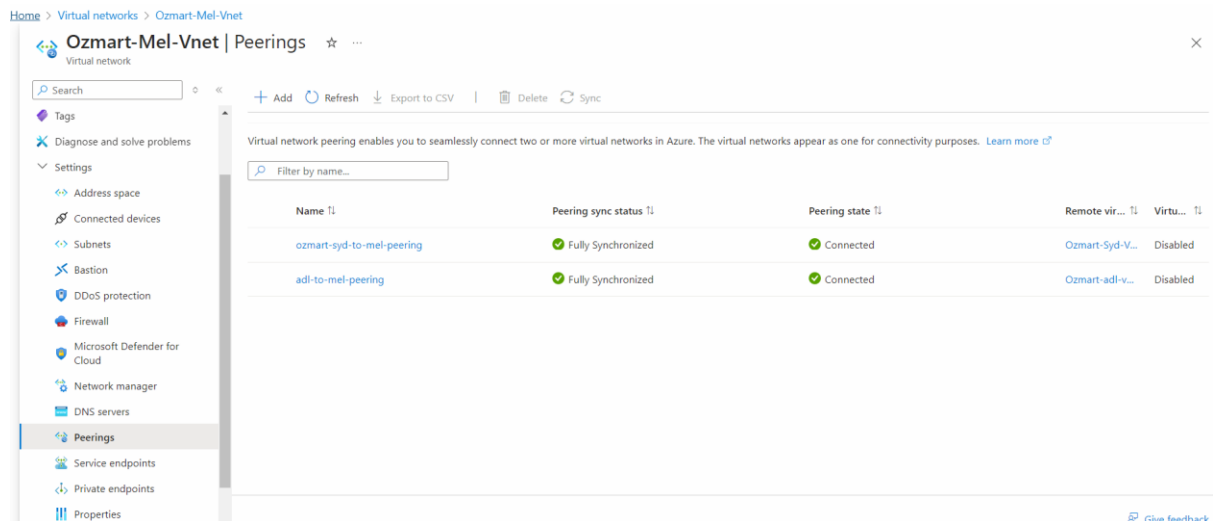


Fig: Vnet Peering

## 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 variety of features that helps in effective management of the network. Traffic management filters inbound and outbound traffic based on the policies 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 an extra layer of security to the subnets. In our environment we have got NSG for Servers and VM's. These help in isolating the traffic to virtual machines and servers further enhancing the security.

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

Home > Network security groups

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 7 of 7 records.

Name	Resource group	Location	Subscription	Flow log
aadds-nsg	Ozmart-Australia	Australia Southeast	Azure subscription 1	
Anupa-vm-nsg	Ozmart-Australia	Australia Central	Azure subscription 1	
Navneet-VM-nsg	Ozmart-Australia	Australia Central	Azure subscription 1	
om-webserver01-nsg	Ozmart-Australia	Australia Southeast	Azure subscription 1	
ozmart-domaincontroller-nsg	Ozmart-Australia	Australia Southeast	Azure subscription 1	
Server-nsg	Ozmart-Australia	Australia Southeast	Azure subscription 1	
Simar-vm-nsg	Ozmart-Australia	Australia Central	Azure subscription 1	

< Previous Page 1 of 1 Next >

Give feedback

Fig: NSG

**Azure Policies:** These help in implementing a standard across the organization. They can play a crucial role in access management and ensure 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.

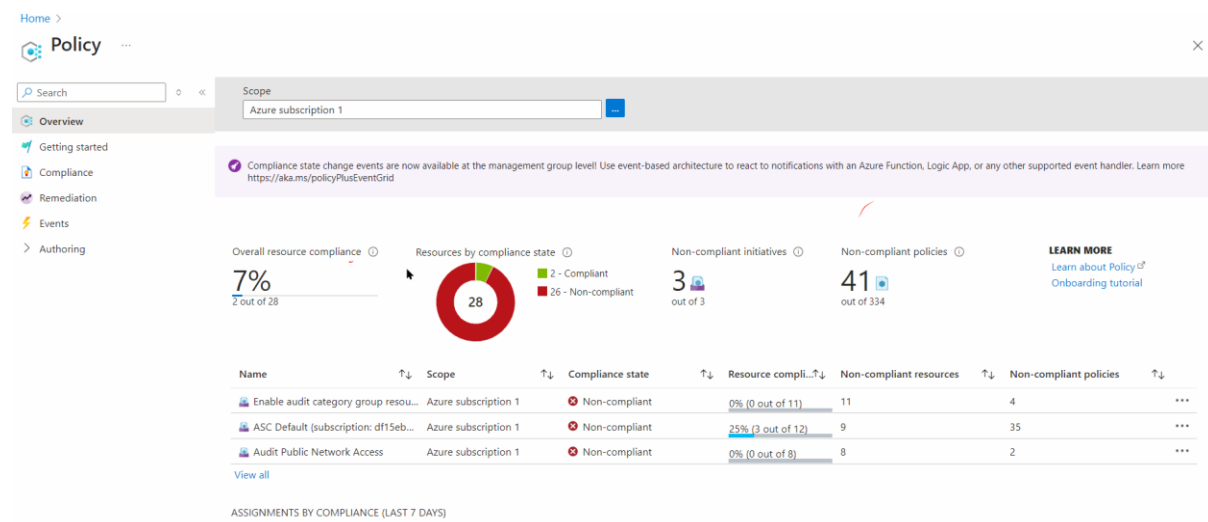
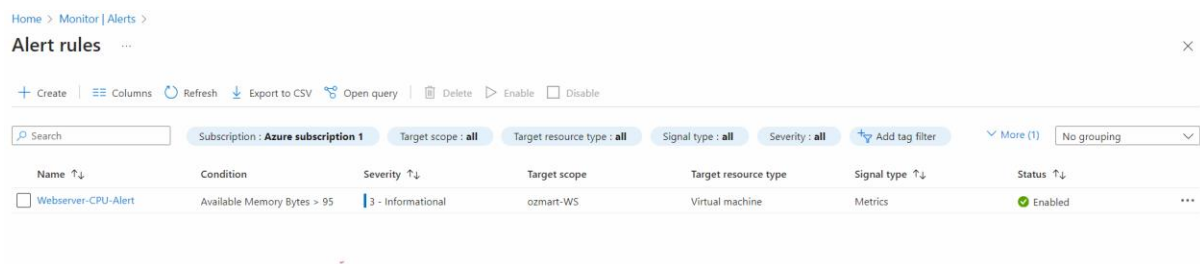


Fig: Azure Policies



**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.



Home > Monitor | Alerts

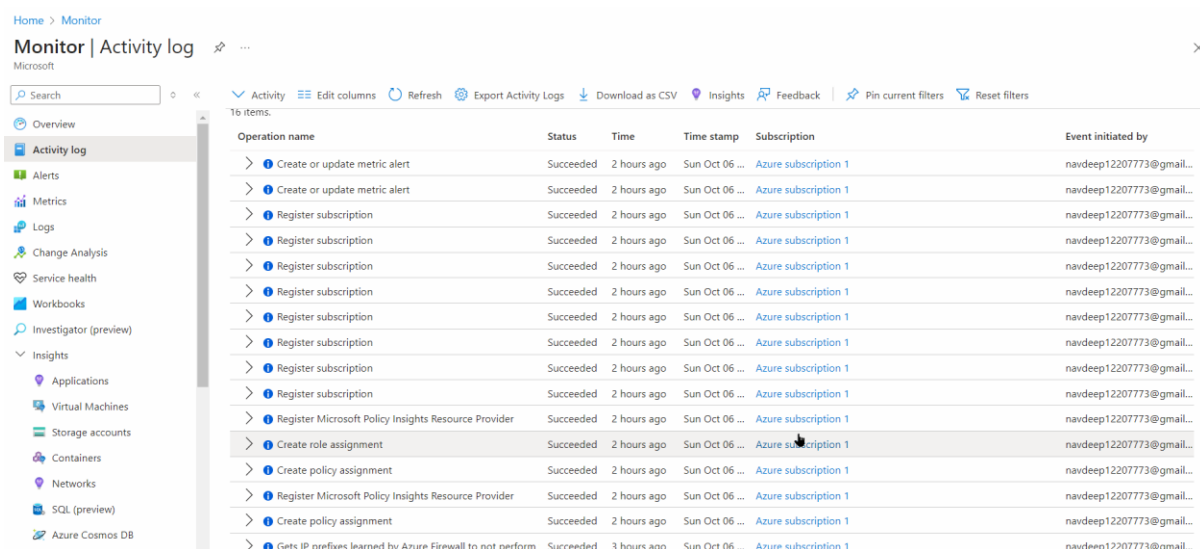
Alert rules

+ Create | Columns | Refresh | Export to CSV | Open query | Delete | Enable | Disable

Subscription: Azure subscription 1 | Target scope: all | Target resource type: all | Signal type: all | Severity: all | Add tag filter | More (1) | No grouping

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
Webserver-CPU-Alert	Available Memory Bytes > 95	3 - Informational	ozmart-WS	Virtual machine	Metrics	Enabled

Fig: Showing Azure Alerts



Home > Monitor

Monitor | Activity log

Microsoft

Search | Activity | Edit columns | Refresh | Export Activity Logs | Download as CSV | Insights | Feedback | Pin current filters | Reset filters

16 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> Create or update metric alert	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Create or update metric alert	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register subscription	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register Microsoft Policy Insights Resource Provider	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Create role assignment	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Create policy assignment	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Register Microsoft Policy Insights Resource Provider	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Create policy assignment	Succeeded	2 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...
> Gets IP prefixes learned by Azure Firewall to not perform	Succeeded	3 hours ago	Sun Oct 06 ...	Azure subscription 1	navdeep12207773@gmail...

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.

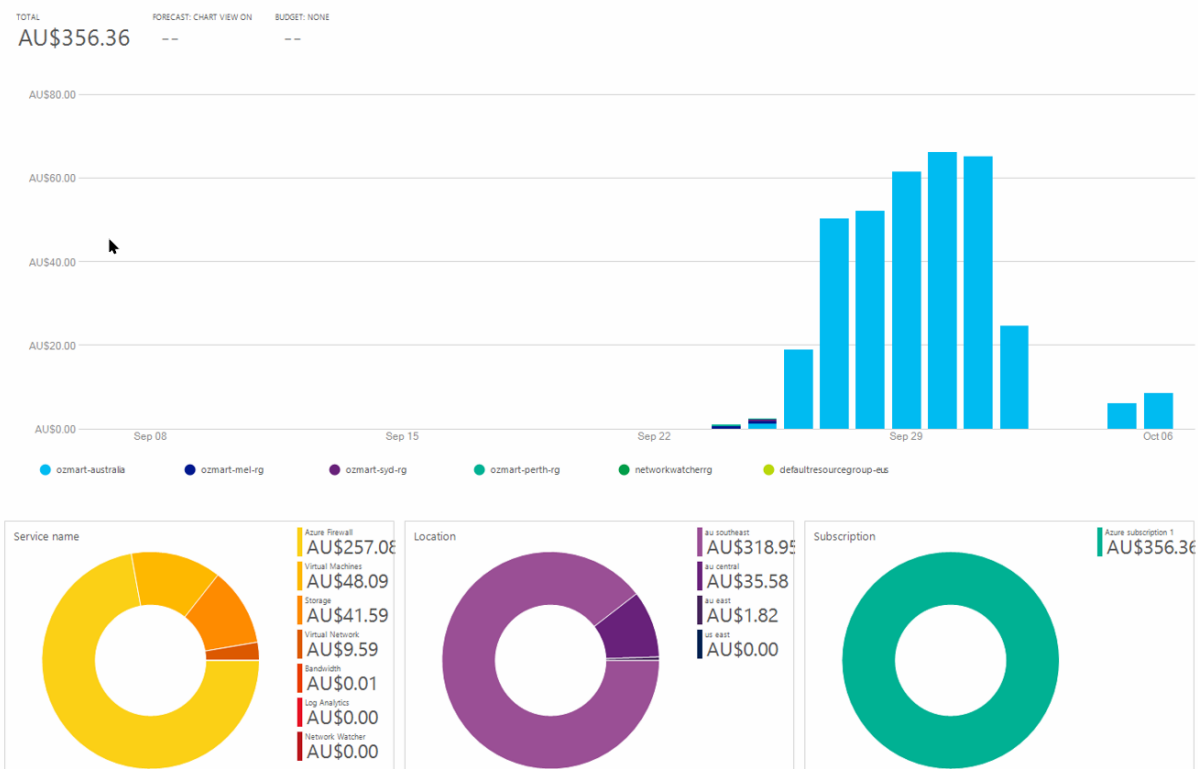
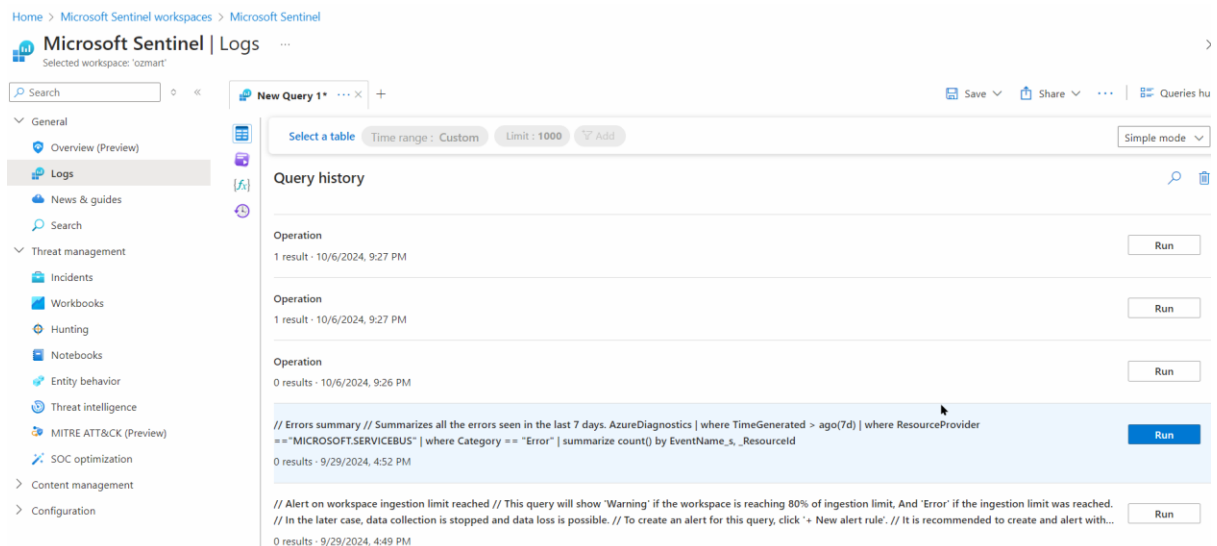


Fig: Cost

**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.



**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.

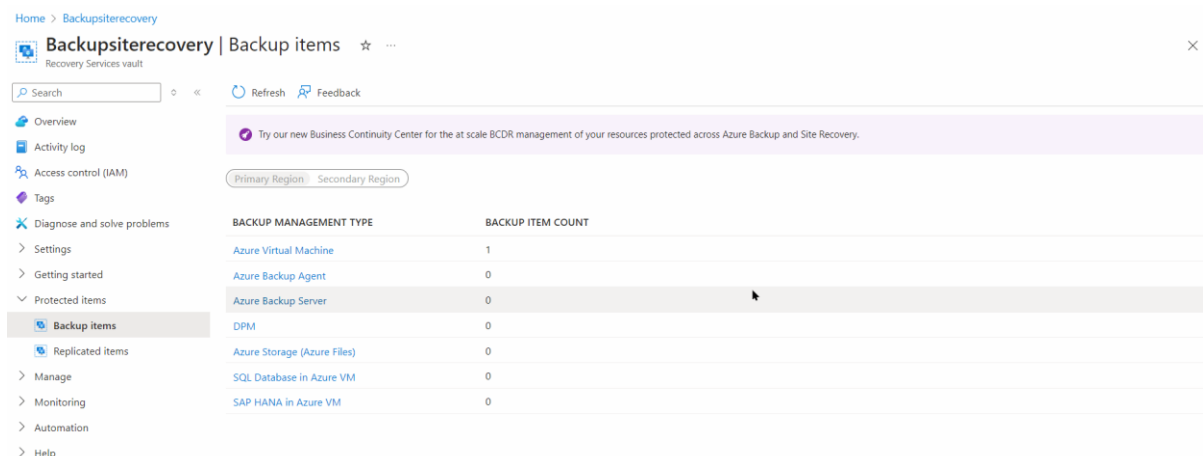


Fig: VM Backup

### 3 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-Instructions.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-Implementation.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	Yes

		to select Azure as their preferred cloud platform.	
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

## 4 Contributions

Student Name	Percent	Summary of Contributions	Technical Lead on Artefacts
<b>Mohmed Amaan Patel</b>	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	<ul style="list-style-type: none"> <li>• Risk Assessment</li> <li>• Risk Assessment Table</li> <li>• Testing and Validation</li> <li>• Problem Statement</li> <li>• Migration Strategy</li> </ul>

		<p>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.</p>	
<b>Navdeep Saini</b>	25%	<p>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.</p>	<ul style="list-style-type: none"> <li>• On- Premises Network Architecture.</li> <li>• Azure Network Architecture.</li> <li>• IP Addressing and Subnetting.</li> <li>• Routing Protocol.</li> <li>• Testing and Validation</li> <li>• Azure Migration.</li> <li>• Monitoring and troubleshooting with cloud tools.</li> </ul>
<b>Simarpreet Kaur</b>	25%	<p>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.</p>	<ul style="list-style-type: none"> <li>• NIST Security Framework</li> <li>• Firewall configuration</li> <li>• Azure Network Security</li> <li>• Azure Migration</li> </ul>
<b>Anupa Bodhimaluwa</b>	25%	<p>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,</p>	<ul style="list-style-type: none"> <li>• Azure Setup</li> <li>• IP Addressing and Subnetting.</li> <li>• Azure Network Design</li> <li>• Review of Existing Cloud Products</li> <li>• Azure Migration</li> </ul>

		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.	

## 5 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.

- 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.
- 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.

3. **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.
  
4. **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.



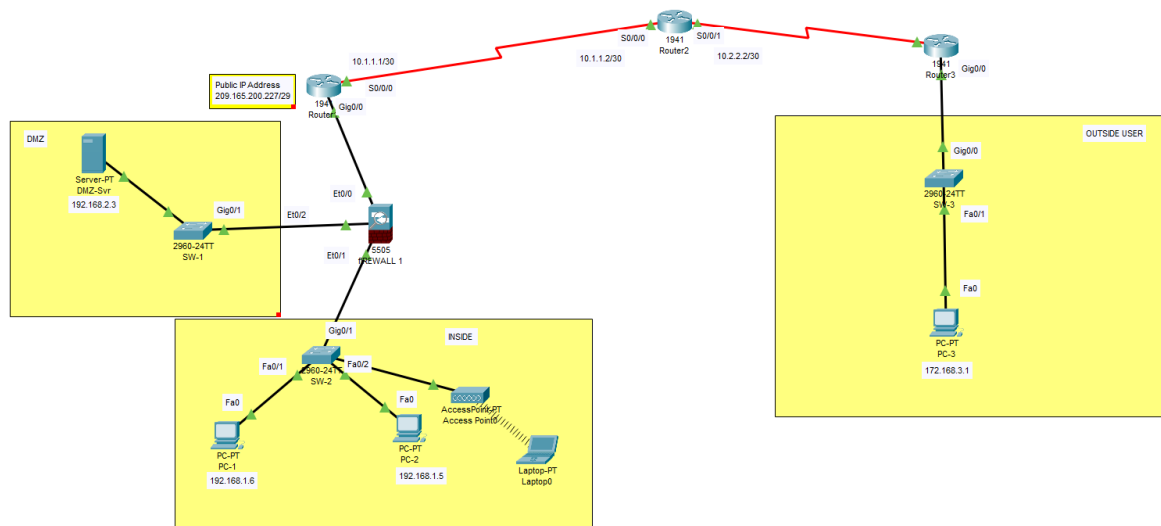
## On-Premises Infrastructure

### Introduction

DEVICE	INTERFACE	IP ADDRESS	SUBNET	DEFAULT GATEWAY
ROUTER 1	Gig0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
ROUTER 2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
ROUTER 3	S0/0/0	172.16.3.1	255.255.255.0	N/A
	Gig0/0	10.2.2.1	255.255.255.252	N/A
FIREWALL	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	N/A
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	N/A
DMZ Server		192.168.2.3	255.255.255.0	192.168.2.1
PC-B		192.168.1.3	255.255.255.0	192.168.1.1
PC-C		172.16.3.3	255.255.255.0	192.168.2.1

Ozmart consist of 2 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.



## 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 OSPF protocol which is used for routing IP packet within Autonomous system. It routes packets using network topology map.

**Firewall:** Firewalls are security devices that are used to protect the network from threat and unknown 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.

## **RISK ASSESSEMENT**

Risk assessment is the process of how to conceptualise and assess the risks. It is critical to assess the risks before migrating to cloud. Identifying the risks will help the team in creating policies which will further help the organisation in minimising the impact and mitigate the risks. In order to identify the cloud risks and analyse them to prevent and minimise the impact Microsoft have recommended below (stephen-sumner, 2024 ):

- **List all cloud assets:** this involves making note of all the assets that will be used in migration, in cloud environment and during migration.
- **Discover cloud risks:** This involves listing all stable catalogue, involves listing frequent adjustment that would be made and noting risks specific to a workload.
- **Involve key stakeholders:** This involves talking to different organisation in order to note all the potential risk
- **Verify risks:** This involves getting experts on board and getting their expertise. These could be experts from cloud provider or 3<sup>rd</sup> part vendors.

Risk-assessment.xlsx includes details of the risk analysis that has been performed by Ozmart IT team. It includes Risk ID, Risk category, Risk description, Risk Level and Risk Management strategy.

In the excel sheet the risks are categorised based on regulatory compliance, Security risk, cost and operational risks. Each risk is associated with Risk ID and includes a brief description. After carefully analysing the risk we have assigned each risk with a risk level that shows the severity of the risk. Finally the last row show the strategy that we will be implementing to mitigate or lower the impact of the risk.

## **REFERENCE**

1. Stephen-sumner (2024). Assess cloud risks - Cloud Adoption Framework. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/assess-cloud-risks#example-risk-list> [Accessed 1 Oct. 2024].

## Azure Setup instructions

### Step 1: Singing into Azure

Launch a web browser and Navigate to azure portal (<https://portal.azure.com>). Click on sing in and Enter Azure account details and Card details. Once logged in you will be redirected to Azure dashboard.

### Step 2: Setting Up Resource Group

In the Dashboard search for Resource group and then click on create and fill out the instruction

- **Subscription:** pay-as-you-go
- **Resource group name:** Ozmart-Aus
- **Region:** Australia Central

[Home](#) > [Resource groups](#) >

#### Create a resource group ...

Basics Tags Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

##### Project details

Subscription \* ⓘ

Azure subscription 1

Resource group \* ⓘ

Ozmart-Aus

##### Resource details

Region \* ⓘ

(Asia Pacific) Australia Central

FIG: Azure Resource group creation

### STEP 3 : Create Virtual Network(Vnet)

In the dashboard search for Virtual network and then click on create. Fill out the instruction as below

- **Subscription:** Azure Subscription
- **Resource Group:** Ozmart-Australia
- **Name:** Ozmart-MEL-Vnet
- **Region:** Australia southeast .
- **Address Space:** 10.0.0.0/16
- **Subnet:** Server(10.10.0.0/26), Laptop(10.10.0.128/26), Management(10.10.0.64/26), Firewall(10.10.0.192/26)

Basics   Security   IP addresses   Tags   Review + create

### Basics

Subscription	Azure subscription 1
Resource Group	Ozmart-Australia
Name	Ozmart-Mel-VirtualNetwork
Region	Australia Southeast

### Security

Azure Bastion	Disabled
Azure Firewall	Enabled
- Name	(New) Ozmart-Mel-VirtualNetwork-Firewall (Standard)
- Public IP Address	(New) ozmart-mel-virtualnetwork-firewall
Azure DDoS Network Protection	Disabled

### IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	server-subnet (10.0.0.0/24) (256 addresses)
Subnet	laptop-subnet (10.0.1.0/24) (256 addresses)
Subnet	AzureFirewallSubnet (10.0.2.0/26) (64 addresses)

### Tags

FIG: Azure Vnet Setup

## STEP 4 : Setting up Firewall

Go back to the dashboard and search for the firewall and click on create. Fill out form

- **Subscription:** Azure Subscription 1.
- **Resource Group:** Ozmart-Australia
- **Name:** Ozmart-Firewall
- **Region:** Australi southeast
- **Virtual Network:** Ozmart-Mel-Vnet.

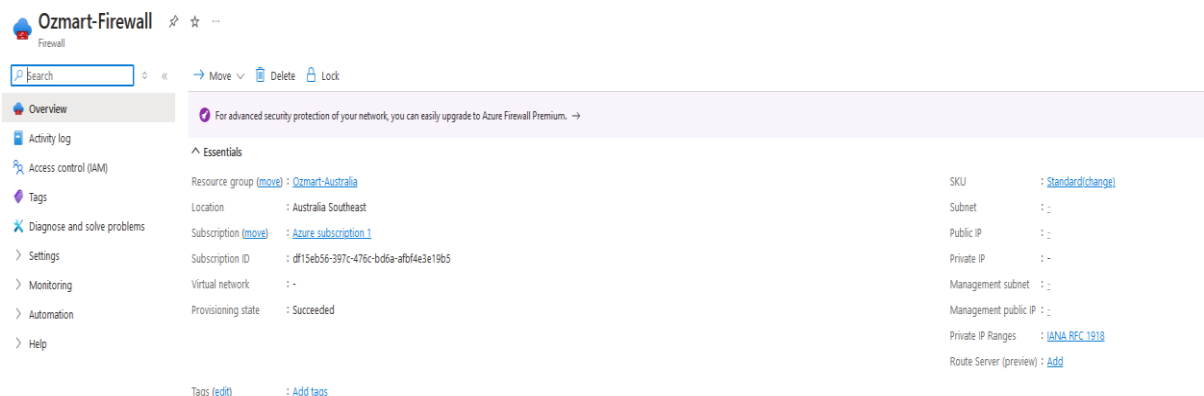


FIG: Azure Firewall setup

## STEP 5 : Create Virtual machine

On the dashboard page search for VM and fill out the form

- **Subscription:** Azure Subscription 1.
- **Resource Group:** Ozmart-Australia
- **Virtual Machine Name:** Anupa-VM
- **Region:** Australia Southeast.
- **Image:** windows 11
- **Size:** 1gb
- **Administrator Account:** amdministrator
- **Inbound Port Rules:** allowing ports like SSH port 22 and RDP port 3389 which are necessary.

To complete, select "Review + create" and then "Create."

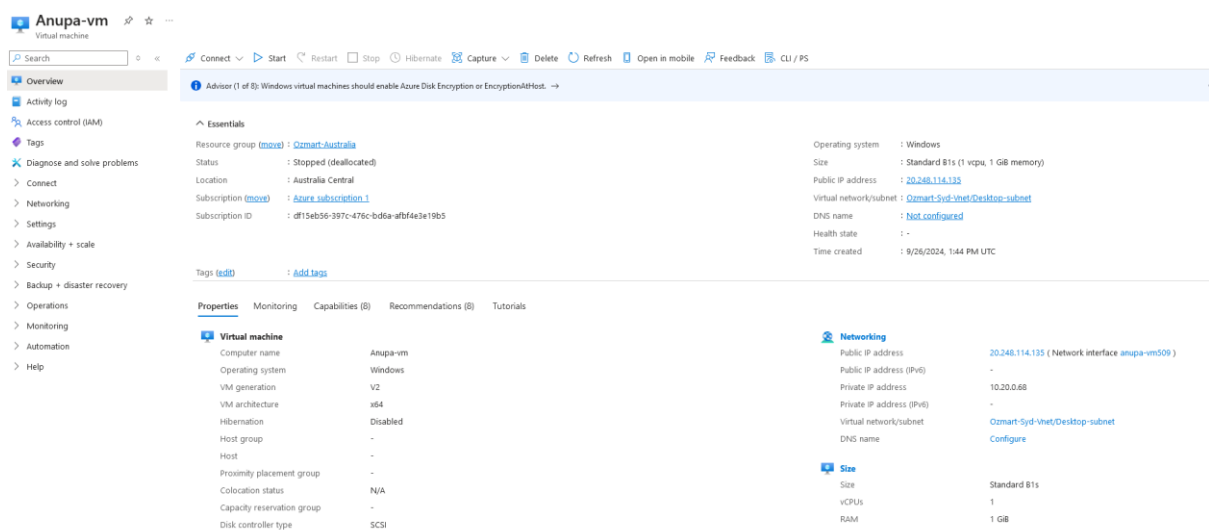


FIG: VM in Ozmart Environment

## STEP 6 : Vnet Peering

Decide which of the two Vnets you wish to peer with. Scroll down to the Peering menu on the left side of the VNet menu and click on it. To start a new peering, click the Add button.

**Fill in the peering details:**

**Name:** Ozmart-Mel-to-Syd-peering

**Subscription:** Azure Subscription 1

**Virtual Network:** Ozmart-Syd-Vnet

**Virtual Network Peering Settings:**

Allow virtual network access: Set to Yes to allow resources in this VNet to communicate with the second VNet.

Allow forwarded traffic: If using a network virtual appliance to mediate traffic between VNets, this option can be set to Yes (if such an option is available).

Allow gateway transit: If the gateway is to be allowed for usage within the peering VNet, it should be set to Yes (if available).



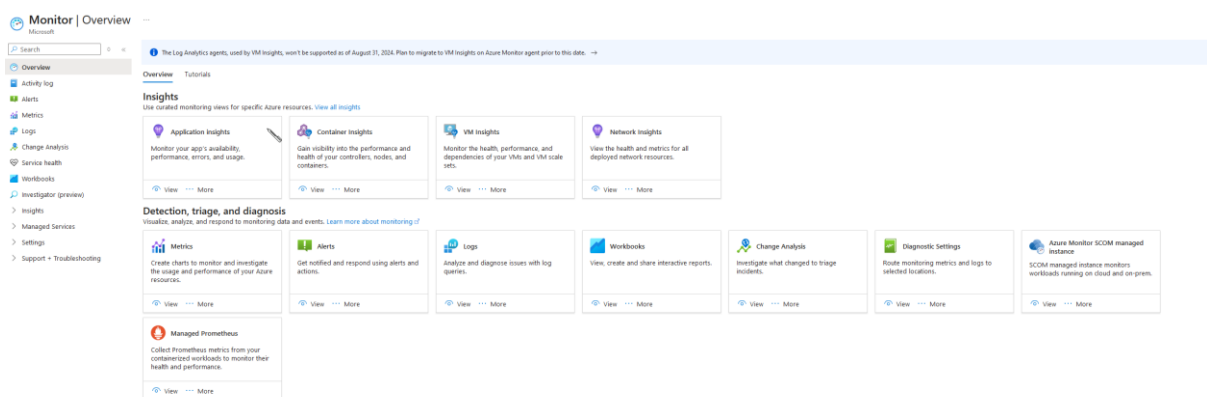
Use remote gateways: Set to No unless you want to use a gateway from the remote VNet.

Click OK to create the peering.

## STEP 7: Handling Resources on Azure

### AZURE MONITOR

Azure monitor is used to monitor resource performance. To access Azure Monitor, put "Monitor" into the Azure portal's search box and select it. Azure Monitor is used to configure different type of alerts. We can utilise metrics section to have graphical representation of the alerts.



### Azure Subscription Management

Bills can be paid on time and there are no backlogs by using the subscription management portal. Look over the subscriptions you currently have. To prevent unforeseen fees, set spending caps and keep an eye on consumption.

### Cost Management

Type Cost Management + Billing in the search bar within the Azure portal and select it. Check out your spending patterns with the help of the "Cost Analysis" tool.



# Migration Strategy

## Lift and Shift (Rehosting):

**Definition:** This strategy entails migrating applications to Azure without having to make any kind of alterations to them. It preserves the original architecture of the code so that transition to the cloud is not a problem.

**Benefits:** Aimed to deploy as fast as possible, introduce minimum risk, and get direct access to the Azure resources.

**Considerations:** Although offering immediate access to the cloud, it may not give the best solution in terms of price and efficiency.

## Refactoring (Replatforming):

**Definition:** This strategy requires getting some optimization for the application due to the environments that are provided in the cloud and other activities which do not change the basics of the application.

**Benefits:** Better efficiency and possibly cheaper than lift and shift if the company will attempt to take advantage of cloud-native capabilities.

**Considerations:** Somewhat more complex than simple lift and shift, though it does require specific development effort and time.

## Rebuilding:

**Definition:** This includes rewriting of the apps from the ground up and deploying cloud-only architectures and services.

**Benefits:** Has the procedures to realize the best opportunities the cloud has to offer regarding feature utilization, size, and structure.

**Considerations:** High risk/start-up cost requires a considerable amount of time and money; ideal for designing over the long-haul vision of cloud.

## Replacing (SaaS):

**Definition:** Here, existing applications are retired and replaced with SaaS that fulfills organizational requirements.

**Benefits:** Frequently results in the accrual of less cost of maintenance and operation.

**Considerations:** Lack of flexibility and the risk to outsource all services.

### **Retaining (Hybrid Approach):**

**Definition:** Some application portfolios remain in the enterprise premises as others are moved to the cloud which makes them a hybrid.

**Benefits:** The ability to keep certain, most likely mission-critical apps on site, while tapping into the cloud for other initiatives.

**Considerations:** Challenges involved in tension and conflict between traditional PD processes and new agile methods, as well as integration issues in a hybrid setting.

### **Lift and Shift Explained**

Lift and Shift is also known as 'wiki building,' and is a common reason why organizations move to the cloud in the first place, since it is swift to execute. Here are some key aspects to consider:

#### **Process:**

Identify the current applications and analyse their interconnections.

Migrate the application and the data to Azure Virtual Machines or Azure Container Services.

As much as migrating the system will give it a new outlook ensure that the connectivity and data is not compromised.

#### **Benefits:**

**Speed of Migration:** Organizations can easily shift loads without a lot of time spent redesigning processes.

**Cost Savings:** Eliminates additional physical equipment expenses while effectively introducing pay-as-you-go characteristics for the cloud.

**Scalability:** The ability to scale up resources when needed on a biased manner.

Challenges:

**Cloud Optimization:** Applications may not leverage cloud cost, may not be optimized for performance.

**Long-Term Strategy:** Lift and shift could just be initial; an organization may well find itself having to do one-time refactoring or outright rewrite for a more resourceful utilization of the cloud. (Jamshidi & Ahmad)

### **Reference**

1. Jamshidi, P. and Ahmad, A. (no date) (PDF) Cloud Migration Research: A systematic review. Available at:  
[https://www.researchgate.net/publication/260420072\\_Cloud\\_Migration\\_Research\\_A\\_Systematic\\_Review](https://www.researchgate.net/publication/260420072_Cloud_Migration_Research_A_Systematic_Review) (Accessed: 06 October 2024).

## Setup Entra ID

When implementing Azure into the Entra ID or what used to be known as Azure Active Directory, then there are several technical artifacts and configurations required. These two integrate mainly to support authentication, identification and security in the cloud platforms. Below are the main technical artifacts and steps required for integration:

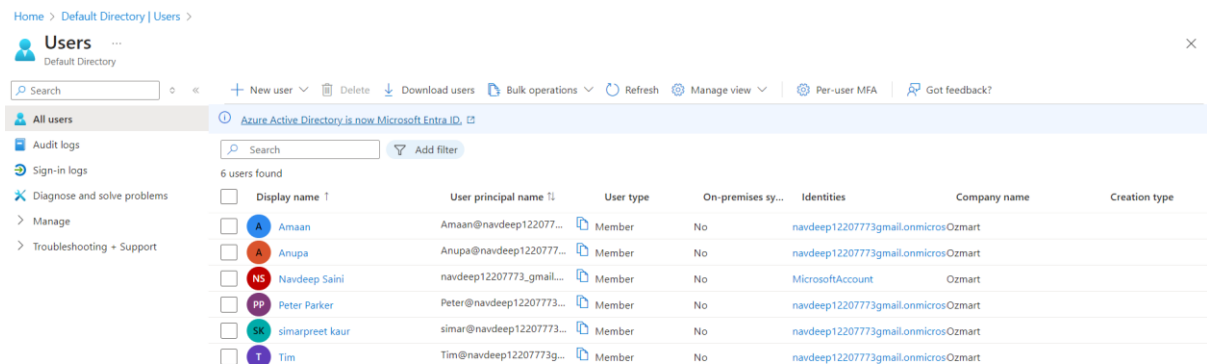


Fig Ozmart Entra ID Setup

1. **Azure Entra ID Tenant** An existing tenant in Entra ID is mandatory to build an integration with Azure resources. This specific tenant caters for the Identity and Access Management (IAM) for users, groups and applications that are in Azure.
2. **App Registration** For applications to connect with Entra ID, it is required that an app registration be made. This registration creates an application (client) ID which is used to refer to the application within the Entra ID.
3. **API Permissions and Consent** The app uses permissions to access several resources in Azure. These permissions are given via the concept known as API permissions. Some of the permissions may be granted if the administrator consents.
4. **API Permissions and Consent** The use of the app entails granting of permissions for accessing the various Azure resources. These permissions are received with the help of API permissions. Some permissions may require admin permission to be granted.
5. **Role Assignments (RBAC)** In order for the service principal or user groups to be able to access certain Azure resources, roles can only be assigned using Azure RBAC. It enables giving the right role to access the right resource.

6. **Conditional Access Policies** Conditional access policies can be set in order to allow to use Azure services. These policies, further set prerequisites through which users or apps can use resources.
7. **Enterprise Applications** When it comes to third party SaaS or on-premises application, you can set up applications in Entra ID Identity as the Enterprise applications to control access, policies and SSO.
8. **User and Group Management** To integrate, one needs to create or synchronize users and groups either by performing online manual work or by synchronizing the Azure AD Connect with the on-premises Active Directory.
9. **Identity Guard and Surveillance** There are other monitoring tools such as Azure AD Identity Protection and Azure Monitor that shall help real-time threat and anomaly detection of users.

## **Cybersecurity Framework**

Cybersecurity frameworks are instruction or guidance outlined for an organisation must follow to mitigate cybersecurity risks. Cybersecurity framework lays the requirement that an organisation adhere to in order to protect their system from malicious attacks. These frameworks are standard and can be followed by multiple organisations (Taherdoost, 2022). Information security standard and Information security Governance are 2 main cybersecurity standards. Networking infrastructure, Hardwares, software and users and information systems are important parts of security standards.

There are multiple cybersecurity standards and framework available to cater to different needs of an organisation. Most commonly used cybersecurity standards are ISO 27000 series, ISF, SOFP, NIST, SOX and RISK IT (Taherdoost, 2022). It is highly crucial for an organisation to understand what each one is based on and select a standard that fits the best for them. However, some organisation will have to select more than one standard in case the needs are not met in one standard.

After doing considerable amount of research we have decided to select NIST framework. Stated below are some information about it and table describing its integration with azure (Taherdoost, 2022):

### **Nations Institute Of Standard and Technology Cybersecurity (NIST) Framework**

In order for a company to rate its maturity NIST provides 3 main components; Core, Implementation tier and Profile (AlShar'e, 2023).

**Core:** The five-essential element of core process that helps in addressing security concerns are Identification, protection, reaction and recovery.

**Implementation Tier:** NIST have a maturity rating scale of 0 to 4 where zero being the lowest and 4 being the highest. These scores are used by the companies to establish a benchmark.

**Profile:** Regularly evaluating security risks and finding maturity level is very important for an organisation. It helps them prepare for the potential security risks that may rise. It also help them determine the priority that they should give to each task in order to mitigate the risk.

### **Strengths of NIST Framework**

#### **Flexibility:**

- NIST can be tailored to adapt to organisation of different size and sector in order to implement customised needs and risk profile (AlShar'e, 2023).

#### **Comprehensive Approach:**



- NIST Framework covers wide variety of tasks including identification, protecting, detecting, responding and recovering from security incidents (Alshar'e, 2023).

#### **Best Practices and Guidelines:**

- The framework offers a strong foundation of best practices that businesses may use because it is built on top of currently in place standards and guidelines (Alshar'e, 2023).

#### **Risk Management Focus:**

- It focuses on risk based strategy to assist companies prioritising their cybersecurity activities according to the specific risk they face (Alshar'e, 2023).

#### **Enhanced Communication:**

- Promotes improved cybersecurity risk and assessment communication between stakeholders, management and technical team (Alshar'e, 2023).

#### **Encourages Continuous Improvement:**

- It helps organisation stay head of new potential threats by promoting a culture of ongoing assessment and enhancement of cybersecurity posture (Alshar'e, 2023).

### **Weaknesses of NIST Framework**

#### **Implementation Challenges:**

- Companies, particularly those with little experience in cybersecurity, may find it challenging to understand and use the framework (Alshar'e, 2023).

#### **Resource-intensive:**

- Smaller firms with tighter budgets may find it difficult to implement the framework as it can take a lot of time and money (Alshar'e, 2023).

#### **Absence of precise measurements:**

- Organizations may find it challenging to statistically evaluate the success of cybersecurity programs due to the framework's lack of precise measurements (Alshar'e, 2023).

#### **Overemphasis on Compliance:**

- The framework's efficacy may be limited if certain firms utilize it exclusively for compliance requirements rather than as a proactive cybersecurity approach (Alshar'e, 2023).

### **Dynamic Threat Landscape:**

- Organizations may find it difficult to keep up with the most recent risks and mitigation techniques as a result of the cyber threats' potential to evolve faster than the framework's upgrades (Alshar'e, 2023).

<b>NIST Function</b>	<b>Azure Service</b>	<b>Description</b>
Identify	Azure Security Centre	Offers consistent threat prevention and security management for hybrid cloud workloads.
Protect	Azure Policy	Assist in the mass evaluation of compliance and the enforcement of corporate standards.
	Azure Active Directory	Offers services for managing access and identification.
Detect	Azure Firewall	Provides identity and access management, encryption, and network protection.
	Azure Sentinel	Intelligent security analytics using cloud-native SIEM and SOAR solutions.
Respond	Azure Monitor	All-inclusive solution for gathering, examining, and responding to data from on-premises and cloud settings.
	Azure Security Centre	Offers advanced threat protection and provides security alerts and incidents.
Recover	Azure Backup	Safeguards your apps and data, making sure you can restore them in the event of loss.
	Azure Site Recovery	Helps maintain company continuity by keeping business apps and workloads operating during disruptions.

## REFERENCE

1. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, [online] 11(14), p.2181. doi:<https://doi.org/10.3390/electronics11142181>.
2. Alshar'e, M. (2023). CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. *Applied computing Journal*, 3(1), pp.245–255. doi:<https://doi.org/10.52098/acj.202364>.

## **PROBLEM STATEMENT**

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 have to 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.