A close-up of a logo

Description automatically generated with medium confidence

**TEMASEK POLYTECHNIC**

**SCHOOL OF INFORMATICS & IT**

**DIPLOMA IN INFOCOMM AND DIGITAL MEDIA**

**ICT SYSTEMS, SERVICES & SUPPORT**

**VIRTUAL DESKTOP TECHNOLOGY (VRDT) CIML015**

**AY 2024/25 OCTOBER SEMESTER**

**PROJECT**

|  |
| --- |
| **Date:**  **“By submitting this work, I am / we are declaring that I am / we are the originator(s) of this work and that all other original sources used in this work has been appropriately acknowledged.**  **I / We understand that plagiarism is the act of taking and using the whole or any part of another person’s work and presenting it as my/ our own without proper acknowledgement.**  **I / We also understand that plagiarism is an academic offence, and that disciplinary action will be taken for plagiarism.”**  **STEPS ID:**  **………….…**    **NAME AND SIGNATURE OF STUDENTS: ………….… ……………** |

Table of Contents

[1.0 Introduction 3](#_Toc168086740)

[2.0 Introduction of Virtual Desktop Infrastructure (VDI) 5](#_Toc168086746)

[3.0 Products selection of VDI 8](#_Toc168086752)

[4.0 Comparison of the changes after implementing cloud 11](#_Toc168086762)

[5.0 Total Cost breakdown 13](#_Toc168086766)

[6.0 References 16](#_Toc168086769)

**Project Report – 30%**

**Requirement: At least 20 page or above.**

**Introduction** – Background, Aim and Purpose of this Proposal

**Intro and Background:**

You are employed in the IT division of Macro Soft, a software training school with six locations around Southeast Asia. According to estimates, their current environment is:  
  
25 employees in management and administration;   
20 IT support staff, 35 instructors;   
800 student developers.   
  
Currently, Ubuntu OS or Windows 10 are given to teachers and students, and they run the following apps:

1) The Libre Office Suite   
2) The Chrome Web Browser   
3) Zoom   
4) The Sublime Text IDE

**Problem statement:**

The employees go around the Southeast Asian branches on a regular basis. Online or in-person, the classes can be dynamic and ad hoc. The IT support team must be able to quickly set up the training environment. When their notebooks or apps malfunctioned, teachers and students frequently lamented the poor response times and lack of technical help. Teachers suffer unnecessary stress as a result, and pupils have a poor educational experience.

**Tasks assigned by Manager:**

To address the notebook or program failure issue, your manager is considering offering a virtual desktop with the required apps pre-installed as a temporary substitute. You are expected to draft and deliver a proposal on this solution to your management.

**Design -** With reference to the above scenario, report on the Virtual Desktop solution for

a. Compute, storage and network requirement;

b. Costing;

c. Pros and Cons;

Product selection – >

**Azure Virtual desktop**

A typical architectural setup for Azure Virtual Desktop is illustrated in the following diagram:

Design diagram – > **Public Cloud**

A screenshot of a computer

AI-generated content may be incorrect.

**Description Product & design Core components**

1. **Dataflow**

The diagram's dataflow elements are described here:

* The application endpoints are in a customer's on-premises network. Azure ExpressRoute extends the on-premises network into Azure, and Microsoft Entra Connect integrates the customer's Active Directory Domain Services (AD DS) with Microsoft Entra ID.
* The Azure Virtual Desktop control plane handles web access, gateway, broker, diagnostics, and extensibility components such as REST APIs.
* The customer manages AD DS and Microsoft Entra ID, Azure subscriptions, virtual networks, Azure Files or Azure NetApp Files, and the Azure Virtual Desktop host pools and workspaces.
* To increase capacity, the customer uses two Azure subscriptions in a hub-spoke architecture and connects them via virtual network peering.

1. **Components**

Azure Virtual Desktop service architecture is similar to Windows Server Remote Desktop Services (RDS). Although Microsoft manages the infrastructure and brokering components, enterprise customers manage their own desktop host virtual machines (VMs), data, and clients.

1. Components that Microsoft Manage

Microsoft manages the following Azure Virtual Desktop services, as part of Azure:

* **Web Access**: By using the Web Access service within Azure Virtual Desktop you can access virtual desktops and remote apps through an HTML5-compatible web browser just as you would with a local PC, from anywhere and on any device. You can secure web access by using multifactor authentication in Microsoft Entra ID.
* **Gateway**: The Remote Connection Gateway service connects remote users to Azure Virtual Desktop apps and desktops from any internet-connected device that can run an Azure Virtual Desktop client. The client connects to a gateway, which then orchestrates a connection from a VM back to the same gateway.
* **Connection Broker**: The Connection Broker service manages user connections to virtual desktops and remote apps. Connection Broker provides load balancing and reconnection to existing sessions.
* **Diagnostics**: Remote Desktop Diagnostics is an event-based aggregator that marks each user or administrator action on the Azure Virtual Desktop deployment as a success or failure. Administrators can query the event aggregation to identify failing components.
* **Extensibility components**: Azure Virtual Desktop includes several extensibility components. You can manage Azure Virtual Desktop by using Windows PowerShell or with the provided REST APIs, which also enable support from third-party tools.

1. Components that we manage

We manage the following components of Azure Virtual Desktop solutions:

* **Azure Virtual Network**: With Azure Virtual Network, Azure resources such as VMs can communicate privately with each other and with the internet. By connecting Azure Virtual Desktop host pools to an Active Directory domain, you can define network topology to access virtual desktops and virtual apps from the intranet or internet, based on organizational policy. You can connect an Azure Virtual Desktop instance to an on-premises network by using a virtual private network (VPN), or you can use Azure ExpressRoute to extend the on-premises network into Azure over a private connection.
* **Microsoft Entra ID**: Azure Virtual Desktop uses Microsoft Entra ID for identity and access management. Microsoft Entra integration applies Microsoft Entra security features, such as conditional access, multifactor authentication, and Intelligent Security Graph, and it helps maintain app compatibility in domain-joined VMs.
* **Active Directory Domain Services (Optional)**: Azure Virtual Desktop VMs can either be domain joined to an AD DS service or use Deploy Microsoft Entra joined virtual machines in Azure Virtual Desktop
  + When using an AD DS domain, the domain must be in sync with Microsoft Entra ID to associate users between the two services. You can use Microsoft Entra Connect to associate AD DS with Microsoft Entra ID.
  + When using Microsoft Entra join, review the supported configurations to ensure your scenario is supported.
* **Azure Virtual Desktop session hosts**: Session hosts are VMs that users connect to for their desktops and applications. Several versions of Windows are supported, and you can create images with your applications and customizations. You can choose VM sizes, including GPU-enabled VMs. Each session host has an Azure Virtual Desktop host agent, which registers the VM as part of the Azure Virtual Desktop workspace or tenant. Each host pool can have one or more app groups, which are collections of remote applications or desktop sessions that you can access.
* **Azure Virtual Desktop workspace**: The Azure Virtual Desktop workspace or tenant is a management construct for managing and publishing host pool resources.

1. Personal and pooled desktops

By using personal desktop solutions, sometimes called *persistent desktops*, users can always connect to the same specific session host. Users can ordinarily modify their desktop experience to meet personal preferences, and they can save files in the desktop environment. Personal desktop solutions:

* Let users customize their desktop environment, including user-installed applications, and users can save files within the desktop environment.
* Allow assigning dedicated resources to specific users, which can be helpful for some manufacturing or development use cases.

Pooled desktop solutions, also called *non-persistent desktops*, assign users to whichever session host is currently available, depending on the load-balancing algorithm. Because users don't always return to the same session host each time they connect, they have limited ability to customize the desktop environment and don't usually have administrator access.

**Capacity sizing and Costings**

Task workload is for students = 800

Knowledge workload is for Staff = 80

Storage calculation:

800 students x 20GB = 16TB

80staff x 50GB = 4TB

Total storage = 20TB

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Total cost for project:**

USD $51k x12months = $612K per year (Example)

USD $14.3K x 12 months = $171K per year

**Pros and Cons:**

**Pros:**

Whether by choice or by happenstance, if your employees are working remotely, sensitive company data will likely be transferred and stored locally at some point, even if only briefly. Even with best practice security precautions, this transfer of sensitive data is risky. Add the variabilities of employees using their own personal devices and networks for work activity and you have a [recipe for disaster](https://www.techrepublic.com/topic/microsoft/).

Azure Virtual Desktop allows employers to deploy virtual machines, configured exactly how they need them to be, that are securely instanced in the Azure cloud. In essence, sensitive company data is never transferred out of the company’s control structure because any data transfers are merely between Azure cloud instances. Within the Microsoft Azure cloud, data is protected by all manner of [built-in security protocols](https://www.techrepublic.com/article/windows-virtual-desktops-how-you-can-manage-monitor-and-virtualise-devices-remotely/), including Azure Firewall, Azure Security Center, Azure Sentinel and Microsoft Defender ATP.

Under Azure Virtual Desktop, access to desktop instances is controlled by conditional access protocols, including [multi-factor authentication](https://www.techrepublic.com/article/two-factor-authentication-cheat-sheet/). Azure infrastructure can be deployed to enable role-based access control (RBAC) and detect threats using Azure Security Center. Azure Virtual Desktop certified compliant with ISO 27001, 27018 and 27701, PCI, FedRAMP High for Commercial and HIPPA.

If your enterprise already subscribes to Microsoft 365 or an enterprise version of Windows, it can establish a desktop instance for each user for free with Azure Virtual Desktop. Therefore, at no extra charge, your remote users can access a ready-made virtual machine running Windows from anywhere, at any time, from any device.

Because Azure Virtual Desktop is managed through the Microsoft Azure Portal, your enterprise can scale desktop instances to meet business needs on the fly. Admins can increase virtual CPUs, add virtual RAM, allocate more virtual hard disk storage, etc., with a few mouse clicks and an admin login account.

**Cons**

The primary caveat to consider when deciding whether to deploy Azure Virtual Desktop for a remote workforce is the quality of network connections. No matter how well you plan and design your virtual desktop instances, they are only worth the effort if your employees have the ability to effectively reach the cloud. Slow internet connections, intermittent connections and no internet connections are all a real possibility and all must be mitigated for cloud-based virtualization to work efficiently.

Beyond the technical aspect of network connections, employers must also consider how much employee training will be necessary. Tech-savvy employees and IT pros will likely have no trouble connecting to Azure and Azure Virtual Desktop servers, but some employees may need at least some instruction to complete the connection. Who will provide that help, how will they provide it, what if it is not effective? These questions must have acceptable answers.

Other questions to be answered include, once in operation, how will employees ask for additional resources if they need them? Will there be a ticketing system with IT department personnel responsible for their resolution? Is that infrastructure in place? Setting up procedures to handle the maintenance of a Azure Virtual Desktop system should be completed before deploying the actual virtual instances.

# 6.0 References

**Azure Virtual Desktop Architecture**

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop>

**Azure Virtual Desktop Cost Calculator**

https://azure.microsoft.com/en-us/pricing/calculator/