Consultancy Report

Author: Umeda Oqilova

1. Introduction

Cloudy Nerds and High Clouds (referred as customer) are merging, which means that they are changing the business strategy with the purpose of unifying these two companies. The leadership of the company has been considering utilizing this transformational time and reorganizing the infrastructure of the companies and locations. They also want to assess if they will benefit from moving to the cloud. This report gives recommendation for the best suited infrastructure while addressing all 'service requirements' given by the customer. The general advice of this report is that hybrid infrastructure, where some workloads reside in On-Premises and other workloads run on cloud, is the most optimal approach for Cloudy Nerds and High Clouds. This hybrid infrastructure approach can address customer's all 'service requirements' mentioned in the document, while building robust security, and cost-effective infrastructure. The report will start by explaining the benefits of the hybrid infrastructure approach, provide an overview of the project plan in the form of Mind Map snip, show the On-premises network topology, recommendation on servers, access control, security solutions and finally describe the benefits of moving to Cloud.

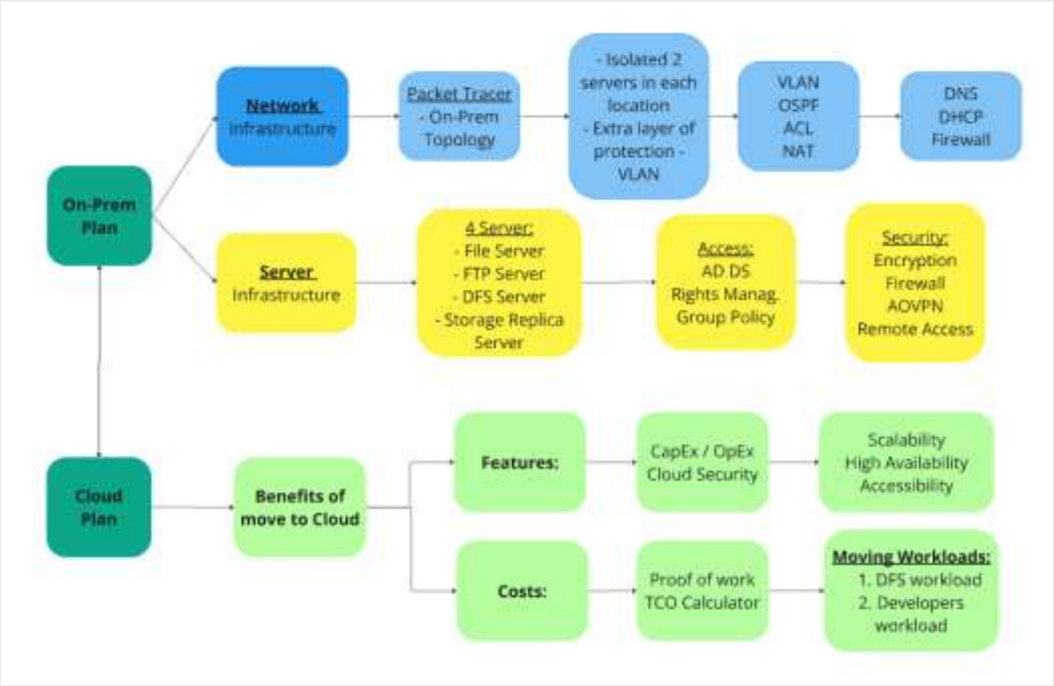
2. Main Part

2.1. Hybrid Solution

Cloudy Nerds and High Clouds are merging and across two locations they have different departments that maintain different services and workloads. These varied workloads are best addressed in hybrid of On-prem and Cloud infrastructure because some of these services and workloads are better suited with On-Prem infrastructure due to ownership, security and compliance of sensitive data, while other workloads are better fitted for utilizing a public cloud like Azure because of operation efficiency, cost effectiveness, scalability and agility. This hybrid approach is flexible and gives the best of both worlds which allows customer to utilize the best IT features in a compliant way with lowest cost. Therefore, the report focuses on different components of the hybrid infrastructure approach that is advised to the customer.

2.1.1. Mind Map

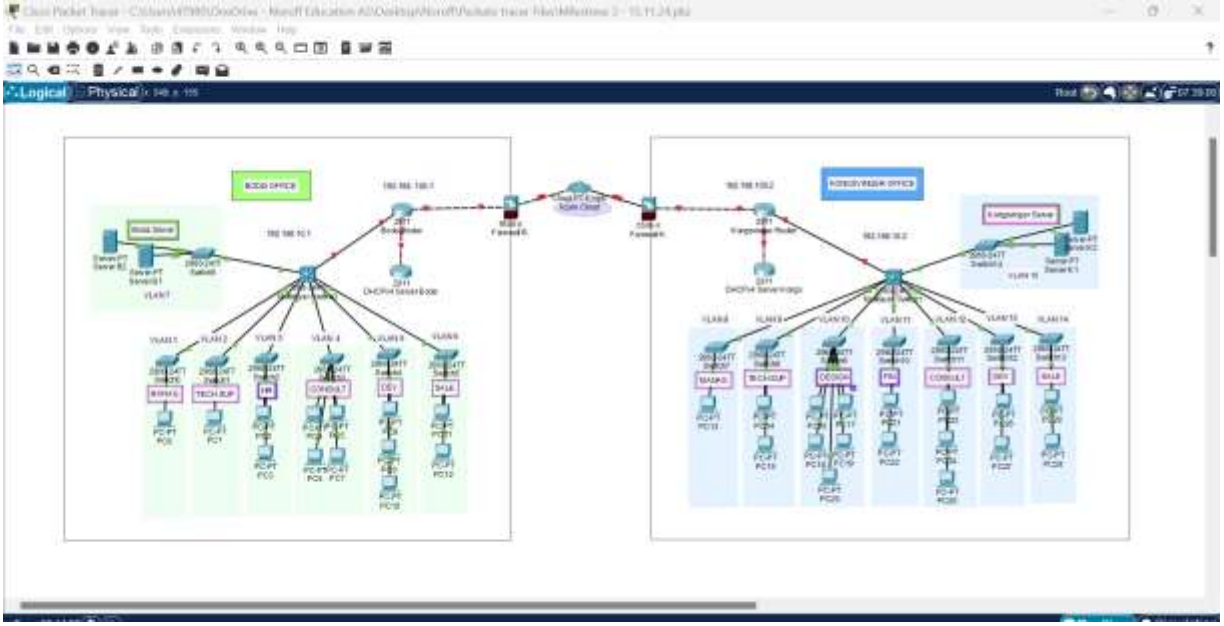
This Mind Map provides a generic visual overview of project plan, describing all of the recommended solutions for the customer in this report. It is divided into two main sections: On-Prem and Cloud infrastructure. Under 'On-Prem Plan', you see network topology in Packet Tracer, isolated servers in both locations and other relevant tools needed for network infrastructure for On-Premises. The other section describes the 'Cloud Plan' and the benefits of moving some workloads to Cloud. These benefits are discussed in two paths: features and costs. The Feature section elaborates on CapEx/OpEx, Cloud Security, Scalability, High Availability, and Accessibility, while cost benefits sections discuss proof of work and TCO calculator by giving examples of two workloads: DFS and Developers workloads.


On-Prem Plan
Network Infrastructure
Packet Tracer - On-Prem Topology
- Isolated 2 servers in each location - Extra layer of protection - VLAN
VLAN OSPF ACL NAT
DNS DHCP Firewall
Server Infrastructure
4 Server: - File Server - FTP Server - DFS Server - Storage Replica Server
Access: AD DS Rights Manag. Group Policy
Security: Encryption Firewall AOVPN Remote Access
Cloud Plan
Benefits of move to Cloud
Features:
CapEx / OpEx Cloud Security
Scalability High Availability Accessibility
Costs:
Proof of work TCO Calculator
Moving Workloads: 1. DFS workload 2. Developers workload

ON-PREM Infrastructure

This on-premises configuration guarantees security, reliability, and scalability while adhering to zero-trust principles and implementing least privilege access. The suggested infrastructure is tailored to meet the unique requirements of each office, facilitating smooth collaboration and preparing for future expansion. Following this, we will delve into the cloud migration strategy to enhance scalability and flexibility. The central section will highlight the technical solutions and technologies needed to address the customer's challenge of securely integrating the two offices.

2.1.2. Network infrastructure in Packet Tracer



This network topology provides a solution for setting network inside each office and connection between the offices in Bodø (High Clouds) and Kongsvinger (Cloudy Nerds). As is shown in the diagram each office is surrounded by separate network borders, multilayer switches, VLANs and servers. These two offices are connected with Router (2911) using WAN that supports strong network connection between two geographic locations. Each office has its own servers which are isolated with VLANs that provide an extra layer of protection by isolating from the rest of internal network to provide additional obstruction from malicious attacks. VLAN isolation is implemented for internal communication and handling access for specific department and/or roles. Furthermore, there are two sets of servers deployed at each location to replicate the data and serve as disaster recovery mechanism. The replication facilitates backup strategy by implementing the site-to-site replication and data recovery. For example, Kongsvinger office' server can serve as a primary role for manage the data, while servers in Bodø office can store replica of data. This ensures that if a server fails, the other servers can seamlessly take over the workload. Configuration in the On-Premises environment is important because it helps with data availability, fault tolerance, and protects the company from service interruptions due to server failures.

The other important element on the On-Prem topology is DHCP routers that help to improve network functionality. DHCP is the technology that appoints the IP address and improves the connectivity of the internal devices. The other important component is Firewall, which serves as a checkpoint for traffic flow, filters it, and protects internal networks from external threats. Moreover, topology depicts the On-Prem network connectivity to Cloud, because the customer is planning to move to Cloud. For hybrid approach, there are many ways to connect internal On-Prem workloads to other workloads running in Cloud. The best practices to connect Cloud and On-Prem are either through internet or through direct private connections. Azure ExpressRoute is a Microsoft solution that provides private connections from On-Prem network to your Azure resources while bypassing public internet completely. The last On-Prem network recommendation is about IP addresses, where the customer is advised to choose IPv4 (over IPv6) since it is best suited for their needs. Some of the above-mentioned technologies are explained in more detail later in the report.

As it is shown in the network diagram above, both Kongsvinger and Bodø offices have their sub segregation that are separated into many departments. For example, Kongsvinger office has seven departments: Management, Technical Support, Design, Finance, Consultant, Developers, and Sales. While Bodø office has six departments: Management, Technical Support, HR, Consultants, Developers, and Sales.

Virtual LANs

Virtual LANs is an important tool in internal On-Prem network because it allows segregation data flow in internal network based on departments. VLANs work by limiting internal network communication consequently optimizing data traffic and blocking unauthorized access to a given subnet. In the customer's case, VLAN serves as a great department segmentation tool that allows HR, Finance, and Design teams to have an additional layer of protection on their subnet. Therefore, the sensitive data travelling in their respective subnet cannot be accessed by any other department employees even if they have access to internal network. This subnet segregation technology enhances security and reduce broadcast traffic.

Access Control Lists (ACL)

The other necessary tool for On-Prem network infrastructure is Access Control Lists (ACLs), which promotes security by filtering traffic and access control using network policies. By using ACLs on network devices will ensure the management the traffic flow, ensuring only authorized departments access sensitive resources. Considering that fact that some departments (HR, Finance and Design) in customer organization deal with sensitive data that others should not have access to, ACL would be a great solution. Limiting access using network policies is a quick and easy solution to utilize for network administrators.

Open Shortest Path First (OSPF)

The other important technology is OSPF (Open Shortest Path First) which helps with powerful and fast connection between the office routers using dynamic routing, and finds the shortest path, hence the name, to connect the office routers. OSPF is very useful technology for dynamic routing between two offices in Bodø and Kongsvinger. This will make sure that the fastest route is established between the devices is established in the other office.

Network Address Translation (NAT)

Another important solution to include for the customer's network infrastructure is Network Address Translation (NAT). NAT focuses on providing internet access to internal devices by translating private IP addresses to Public IP addresses. The other component of it is Port Address Translation (PAT) that gives multiple internal devices the same public IP address, hence masking the internal IP addresses. (On-Premises. AW06). These masking of internal IP addresses can serve as an additional layer of protection for potential network targeted hacking. NAT is an important tool to secure internet access and IP address conservation between offices and external resources. It is a very important component of the network infrastructure for companies running IPv4, which we will discuss in the next paragraph.

IPv4

Even though it is generally advised for new companies start with or transition to IPv6 due to lack of IPv4 addresses, we advise Cloudy Nerds and High Clouds to continue using the IPv4. The benefit of remaining in IPv4 is outweighing the transition to IPv6. One of the biggest reasons is that it is not cost effective for the customer to transition to IPv6 at this time. The reason being that transitions will require upgrading hardware or buying IPv6 compatible devices which can have hefty cost attached to it.

The other reason is that two arguments for transitioning to IPv6 (being scarcity of IP address and routing efficiency) are not so relevant to customers' problems. Let us assess these two arguments, first being is the '*Scarcity of IP addresses*' – which is not so relevant to the customer because they are small size of startup company did not require a large number of IP addresses. As was mentioned earlier, NAT is a great tool that can help with making internal IP addresses. Also, the lack of IP addresses could be resolved by incorporating a private address range which could be sufficient until the customer reached the enterprise-sized company and obtained a bigger budget. The second argument is '*Routing efficiency*', which is important to the customer, but this efficiency can also be reached using IPv4 in combination with OSPF. This means that even though transitioning to IPv6 has its benefits in general, it is not necessary for the customer's case because the benefits of IPv6 could be reached by combining IPv4 with OSPF and NAT without added cost for updating hardware devices. Using IPv4 is the best practice for companies with a smaller network that does not require separate IP addresses for every device.

DNS

When creating On-Prem networks infrastructure it is important for a company to have a Domain Name System (DNS), because it is a tool that helps to translate IP addresses into internal network devices to a human readable domain name, like a website. It helps to convert and recognize IP and domain name hence enabling interaction of internal resources with external clients. Given the customers case scenario, it is important to utilize this technology in both offices to translate website names to IP addresses and allow easy communication across all devices in network and external end-users (Krause, 2021). By implementing centralized DNS, the customer will facilitate easy communication and simplified IP translation and domain name across the internet.

Cloudy Nerds and High Clouds have predominantly an On-Premises environment and maintaining existing system as primary solution is important because it can efficiently handle internal solution for core services such as FTP and DFS. Having said that Azure DNS can seamlessly integrate into On-Prem DNS and compliment with sustaining the less important external workload like public-facing sales website. This hybrid approach allows the company to benefit from Azure DNS for cloud-specific workloads while avoiding the complexity and cost of a full DNS migration, ensuring secure, reliable, and cost-effective connectivity across both environments.

DHCP

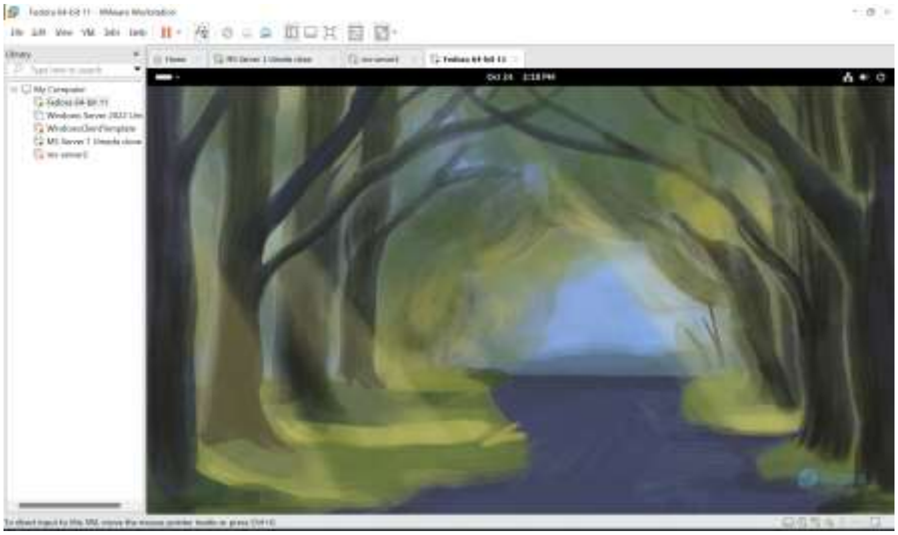
The other important network tool the On-Prem infrastructure requires is Dynamic Host Configuration Protocol (DHCP). It serves as a network protocol that automatically assigns IP addresses to devices within a network. This protocol takes away manual configuration and gives a unique IP address to each device. It also gives necessary network settings like default gateway and dedicated DNS server that makes integration process automated. It can also serve as a security layer by hiding the IP addresses from internal devices and show only one public IP address. This was external user will see only public IP address and protect internal network devices (Rob, 2022).

DHCP is an important tool to implement for network infrastructure of Bodø and Kongsvinger offices because it allows efficient IP address management for all devices, VLANs ensuring that all devices have appropriate network setting. It also grants public and private IP address management for the offices serving as an additional security layer (TechAcademy, 2022). DHCP is simpler to manage with IPv4 because of dynamic IP assignment that helps control network devices and scale the network growth. It also can establish a support system that allows for easy configuration of department/VLANS that is aligned with customers' zero-trust security model and least privilege methods. The easy integration of IPv4 to VLANS is relevant for customers' circumstances where access to data should be controlled through roles, department, and office. It is advised that the customer chooses IPv4 with DHCP because it provides simpler setup, flexibility to control network devices, zero-trust compatibility, and lease privilege to department and office locations. It also provides security by implementing the configuration of IPv4's DHCP, VLAN, and NAT, which makes it the best choice for small companies trying to merge (Rob, 2022).

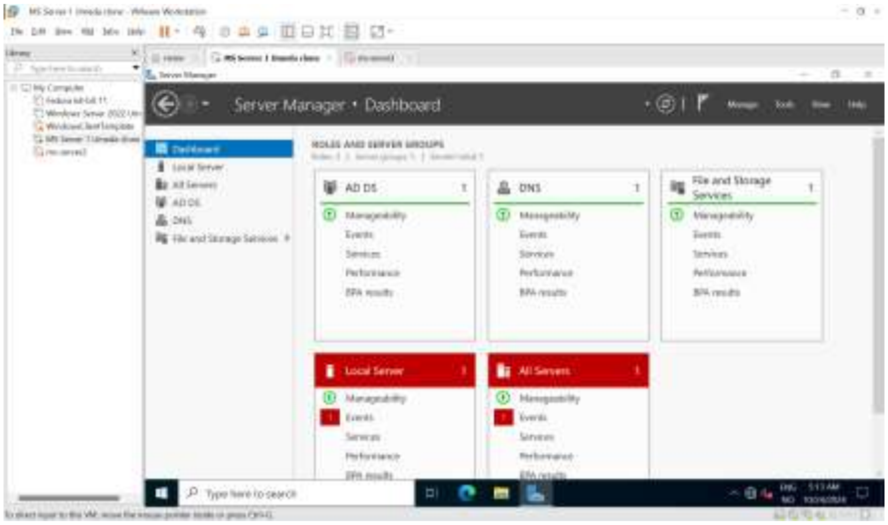
2.1.3. <u>Server Setup:</u>

It was mentioned by the customer that some departments would like to use both Microsoft and Linux server systems for some of their various On-Prem services. Customer's network administrator can easily create virtual machine (VM) inside VMware Workstation (or any other preferred tool) and install Windows Server or Linux operating system (OS) Fedora distribution on top of VMs. That way VM can have Graphical User Interface (GUI) or typical user interface for ease of use and management. Here is the how Windows Server or Linux operating system (OS) looks like on top of VM.

See below for Linux Fedora



See below for Microsoft Windows



This operating system serves as a core solution that allows the network administrator to use server manager and many other tools to regulate the environment by installing, configuring/managing the servers and monitoring the workload and access to data.

File Server

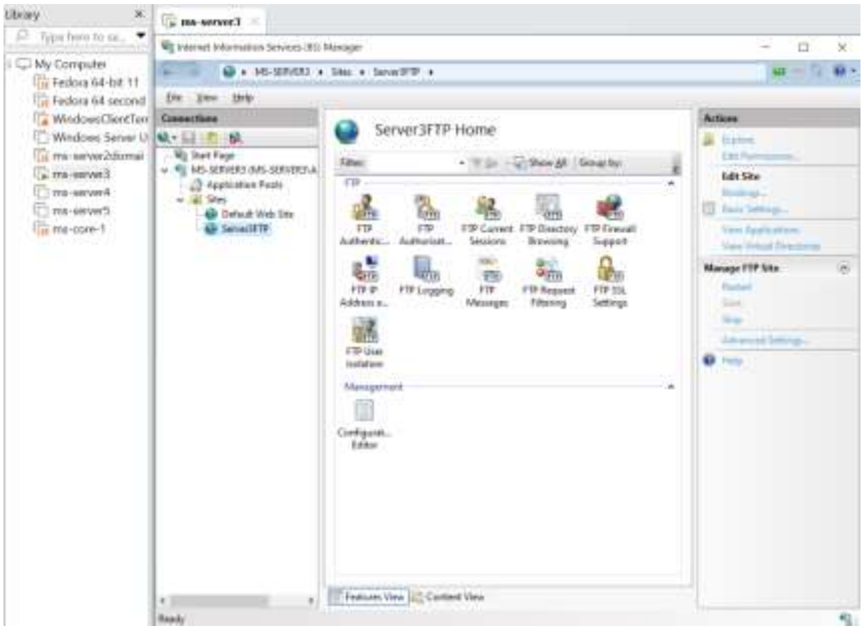
File server with storage service is a backbone of both On-Premises and Cloud infrastructures. In many cases, it serves as a glue that unifies data storage and data management by providing centralized system for a company with many locations and remote work policy. Since the main goal of the customer is merging two companies with two different systems, Windows File Server is a great solution that will serve as a unifying file sharing system that enables secure sharing of files across locations, efficient access control, and combined resource management. In the case of Cloudy Nerds and High Clouds, it is essential to merge their existing separate file systems into one centralized system for ease of data management, better communication and collaboration between the employees.

Windows File Server allows to add the New Technology File System (NTFS) permissions which is essentially an access control setting in Windows that defines which users or groups can Read, Write, modify, or execute files and folders on an NTFS-formatted drive. And system administrators can use NTFS permissions to define the access level to correct employees (Microsoft, n.d.). For example, an administrator can grant full control to consultants, while the design team can get Write access, meanwhile Read-only access is given to the sales team. This will make sure that the right access is given to the right team, hence preventing accidental or unauthorized edits of the important files. The File System is at the center of the company's data management and seamlessly connects to key solutions such as File Transfer Protocol (FTP), Distributed File System (DFS), Storage Replica etc., which are discussed in detail below.

FTP Server

For the On-Premises environment of the customer, it is advised to implement the File Transfer Protocol (FTP) because it is a great communication protocol that allows file exchange between the client and the server. It can establish the connection between the users and send big files between client computer and servers remotely or within the local network (Microsoft, n.d.). Essentially, FTP facilitates client to connect and send commands to server and get its' reply. As it is mentioned under the service requirement of the Cloudy Nerds and High Clouds, the design team uses FTP site for sharing design templates with assumingly large files (Kinsta, n.d.). FTP has client authentication and authorization that allows/limits the permission of the user to access the FTP server and download files. In the case of Cloudy Nerds and High Clouds, the design team could use FTP dashboard to manage design templates, control the access and prevent unauthorized download or changes to the template.

FTP is a convenient tool, but it might have some security concerns such as not encrypting the data over the network. This can be addressed by implementing the access control lists (ACLs mentioned above) and using File Transfer Protocol Secure (FTPS) to encrypt data in transit over the network, unauthorized access and data interception. An additional layer of security could be implemented by keeping the design templates off the public internet and allowing access through only internal network or through secure VPN. To meet the requirements of the design team mentioned under the service requirement, it is advised to utilize the role-based permissions that will give them permission to modify and upload new files, meanwhile all other employees can have read-only access to templates. The below snip provides an overview of the FTP dashboard that design team can use to manage and tailor the access level to their templates and share them with the rest of the company easily without compromising on security.



Distributed File System – DFS

Distributed File System (DFS) serves as an important solution to replicate file shares, organize and control access to important files. In the case of Cloudy Nerds and High Clouds, DFS can help to create centralized namespace that will be a unified folder structure for both Kongsvinger and Bodø offices. This will allow employees access and work with common files without worrying about the physical location of the data or making sure that other offices get updated copy (Microsoft, n.d.). DFS provides crucial solution for the customer, because they deliver various IT services which require input from different teams such as developers, design, technical support and consultant to work simultaneously on various files. It is this simultaneous work on files that required consistency and accessibility to ensure seamless collaboration and productivity.

The essential component of DFS is replication between two servers which ensures availability of the file system and increased possibilities for data Writes. It allows the users one path for access files regardless of the server data stored on. It also has automatic updates that allow synchronization across the servers. DFS system handles Write conflict, which means it can handle multiple people working (writing/editing) on the same files without causing an issue. This synchronization is critical for customer's case who have two office locations, remote workers and need for cross team collaborations. That is why DNS is advised as an essential tool for the Cloudy Nerds and High Clouds because it ensures seamless synchronized workflow, automatic redirection of server hosting and reducing the downtime.

The other relevant component of DFS is controlling access to specific files. As it was highlighted under service requirements by customer, their consultant should have full control since they are responsible for the whole DFS system. Full control can be implemented by giving administrative control since consultants supervise and maintain all technical aspects of DFS system and keep it up to date. Meanwhile, the design team can have Write access for DFS permissions to configure those files because they need to update/change files. However, they should receive Read-only access to technical how-to-document, which ensure the viewing privileges without allowing accidental modification or deletion of critical files. Least access tier in the DFS system is given to the sales team because they need to view the files only for reference purposes but are not responsible for making edits. By granting sales with Read-only access, we will give access to updated information for them to perform their task, while protecting accidental modification of the document.

DFS is an important tool for the Cloudy Nerds and High Clouds, since it creates the synchronized file sharing system that provides the exact level of control to correct teams. DFS's tailored permission feature and replication of data across servers make it a mandatory solution that meets customer's security goal and lease privilege access objectives.

Storage Replica – Fault Tolerance

The main task of Storage Replica (SR) is, as name suggests, to replicate the data in On-Prem Windows server to another server. SR ensures that a back-up copy of data is quickly synchronized and saved in another location in case of attacks, data loss, server failures, natural disaster etc. SR replicates the data across the servers, sites and databases on the block level that encompasses the whole storage drive of the company data (Microsoft, n.d.). This feature provides fault tolerance by ensuring that services continue running seamlessly even when a failure occurs at the primary site. This is a good tool to make sure that company data is synchronized (writing data both in both sites simultaneously) across the teams and locations. It also supports asynchronous replication, where the company has a primary site and data is written on that site first and then replicated to secondary site with a slight delay.

As it is shown in the network infrastructure, each location (Kongsvinger and Bodø) has servers that can replicate that data in the other location and serve as disaster recovery solution. Cloudy Nerds and High Clouds can implement back-up strategy by setting up site-to-site replication and making sure that if the data is lost in one location, the secondary location can provide the latest copy and take over as primary storage system. This configuration adds another layer of fault tolerance, protecting the company from service interruptions due to server failures. As the customer is aiming to set up and configure their system with 98.5% uptime, this storage replication provides the fault tolerance needed to meet that goal and minimize service interruption. Replication of the storage system is essential because if the customer loses data for any unforeseen reason, they can still continue providing services since the secondary server will take over the workload of the primary server (Microsoft, n.d.).

Availability of the data is another important point that Storage Replica addresses with synchronization of the files. It can keep the file configurations for sensitive customer data in synchronization across both locations, allowing IT Teams to perform maintenance on the one location while the other remains fully functional, and maintaining the workload for both locations. This ensures that the company can continue its services without outage. Their webpage will remain functional with minimal delays, and sales file / other sensitive data will always be accessible. This setup reduces the need for manual back-up process or troubleshooting of server crashes and data loss, which in turn allows system administrators to focus on more important tasks. As per our advice on establishing a hybrid environment, it is recommended that customer keeps sensitive data on the On-Premises because of security and compliance reasons, while moving the less important data to Cloud environment due to its affordability. More information on moving some data storage to cloud and its benefits will be discussed in the second half of the report, under the DFS System workloads section.

2.1.4. <u>Access Rights Recommendations</u>:

Services and tools like Active Directory Domain Services (AD DS), Rights Management, Active Directory Rights Management Services (AD RMS), and Group Policy do not necessarily require a dedicated server. Instead, they can be integrated and configured on existing servers within the on-premises environment. This allows these tools to efficiently manage various workloads running on the same servers, streamlining operations without adding unnecessary infrastructure complexity.

Active Directory Domain Services (AD DS)

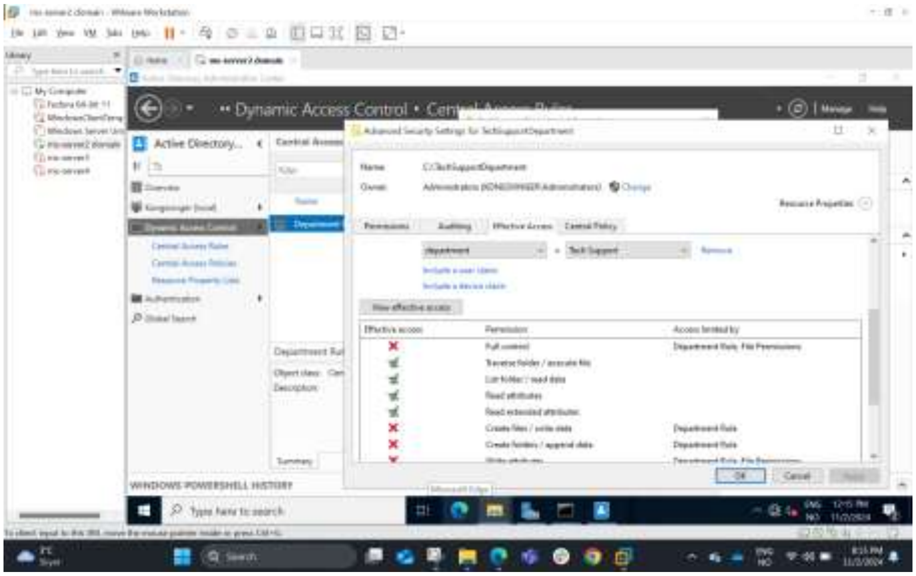
One of the important steps of creating an On-Premises environment after setting up the server OS is to create unified user domain for all employees. The domain servers usually serve as storing directory data and storing data such as user accounts, names, passwords, phone numbers and other relevant employee data. This can also synchronize with other AD and authentication tools that manage access to data. In the customer's case, it will be important to merge and unify the User Domain of Cloudy Nerds and High Clouds employees, because without it system will see employees from the other location as external users. One of the excellent tools that can help with that is Active Directory Domain Services (AD DS), which can serve as a management tool that controls user identity, group policies, and grant/deny permissions to the local network. AD DS is an essential tool for network administrators that helps them to regulate access control over the employees based on their roles in the organization (Krause, 2021). Considering the fact that Cloudy Nerds and High Clouds are trying to enforce zero-trust security model based on user roles and focus on lease privilege access approach, AD DS is a must-have tool to implement those goals.

AD DS manages user access and permissions to local network resources through authentication based on access policies. AD DS gives administrators unified control over the network to apply security policies, manage user accounts, and regulate group policies. AD DS can help customer to build their centralized authentication or their users and assign permission based on their departments. In the case of the Cloudy Nerds and High Clouds, AD DS can serve as an important unifying domain server that can simplify the management of complex On-Prem infrastructure of merging company with many departments with various permissions.

Rights Management

One of the important objectives that Cloudy Nerds and High Clouds are trying to implement is a zero-trust security model with a focus on the least privileged access to data. Groups policies and rights management play an important part in implementing that zero-trust model. Rights Management helps to secure data by regulating - access control, usage restriction, persistent protection, and identity verification. For example, it identifies whether the user has access to Read, Write and Execute the given file or document. Usage restriction goes even further but controlling what can be done with document or file after 'access' is given. It focuses on managing whether the user can edit, copy, print, or share the document/file. Persistent protection is about continues protection of the file even after it is passed around. Identity verification focuses on making sure the use is authorized and implementing authentication process to verify identity and permission levels. This fine-grained control over file access will ensure that employees have only the minimum necessary access to a file. One of the best tools that leverage right management in AD servers is Dynamic Access Control (DAC). DAC helps to implement the rules base conditions like user's roles, departments, and/or location. It is an excellent solution for the customer since it was highlighted in their service requirements that access control will vary based on roles, department, and locations. One of the examples is that the Technical Support team are running the internal website, and they have full control over the page, but all other employees should have Read access to view the site.

See below for Dynamic Access Control. See the picture below for easy user interface to grant access.



Advanced Security Settings for TechSupportDepartment

Name: C:\TechSupportDepartment
Owner: Administrators (KONGSINGER\Administrators)

department = Tech Support

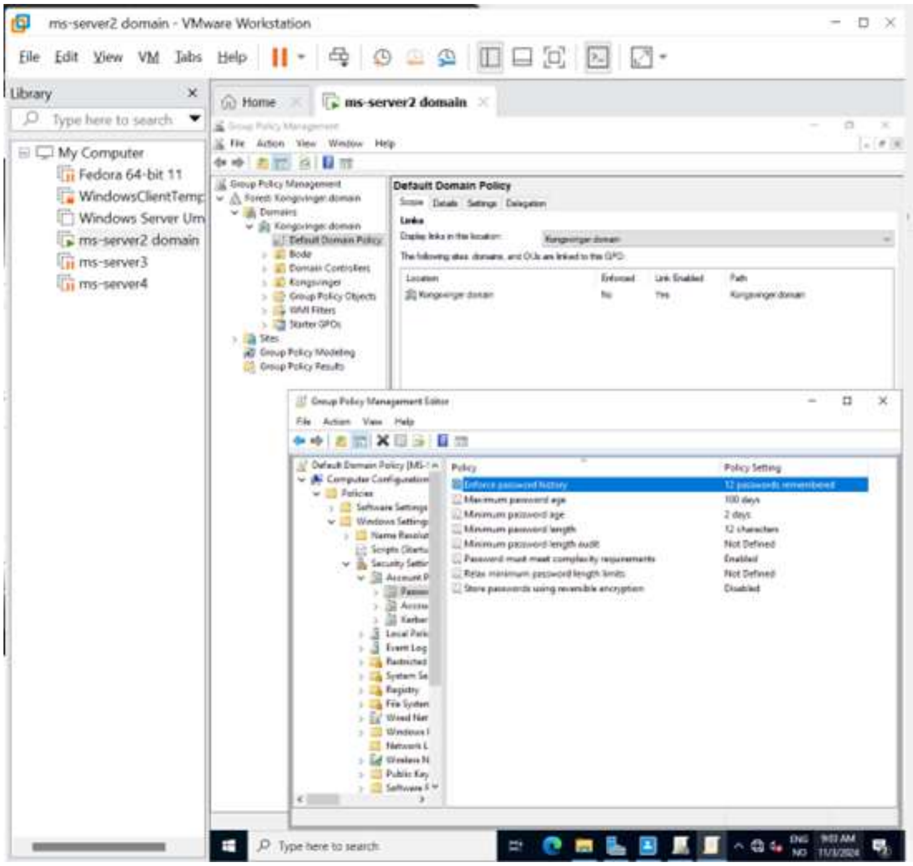
Effective access	Permission	Access limited by
✗	Full control	Department Rule, File Permissions
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	
✗	Create files / write data	Department Rule
✗	Create folders / append data	Department Rule

Group policies

Group Policy is a great management tool in an On-Premises environment that helps to control the setting for all items (computers and users) withing the internal network. It allows administrators to automate identical sets of policies and settings to all users by creating a rule (policy) and apply it to all users, specific group/s or individual users. Group Policy Objects (GPO) is the actual rule administrators create and specify the settings before 'linking' (applying) them against users or computers. For example, GPO can create templates that provide shortcut pathways for administrators to manage the system without manually creating every single policy and settings. For example, creating GPO that can enforce a strong password, often password change and automatically install relevant software for different departments. Automatic enforcement of strong password across all network users reduces the risk of getting hacked, especially when they are using the corporate network remotely (Liberman, n.d.).

Cloudy Nerds and High Clouds care about security but require remote access for some users from the Management, Consulting and Sales departments. To solve these challenges, network administrators can enforce installation of VPN policy for these groups, hence ensuring secure remote access to company data which we will discuss in detail at later paragraphs (Liberman, n.d.). But the important thing to know about Group Policy is that it helps administrators to configure a strong password policy across all users in both locations that work hand in hand with security tools like remote access. Considering the fact that HR, Finance and Design teams handle sensitive data, network administrators can impose an additional layer of security by creating a policy enforcing the physical presence to employees from HR, Finance and Design teams due to localized operation and blocking any remote access. Below you can see a snapshot of strong password group policy as proof of concept.

See below the Groups Policy



ms-server2 domain - VMware Workstation

Default Domain Policy

Links

Display links in this location: Kongsvinger domain

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Kongsvinger domain	No	Yes	Kongsvinger domain

Group Policy Management Editor

Policy	Policy Setting
Enforce password history	12 passwords remembered
Maximum password age	100 days
Minimum password age	2 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

2.1.5. Security Recommendations:

Security is the forefront agenda of the IT companies; it is important to find a suitable security solution for the On-Premises network system that is both reliable and inexpensive. So, to build a secure and manageable infrastructure that supports zero trust and least privileged access, it is advised that the customer implement the above-mentioned security tools.

Encryption

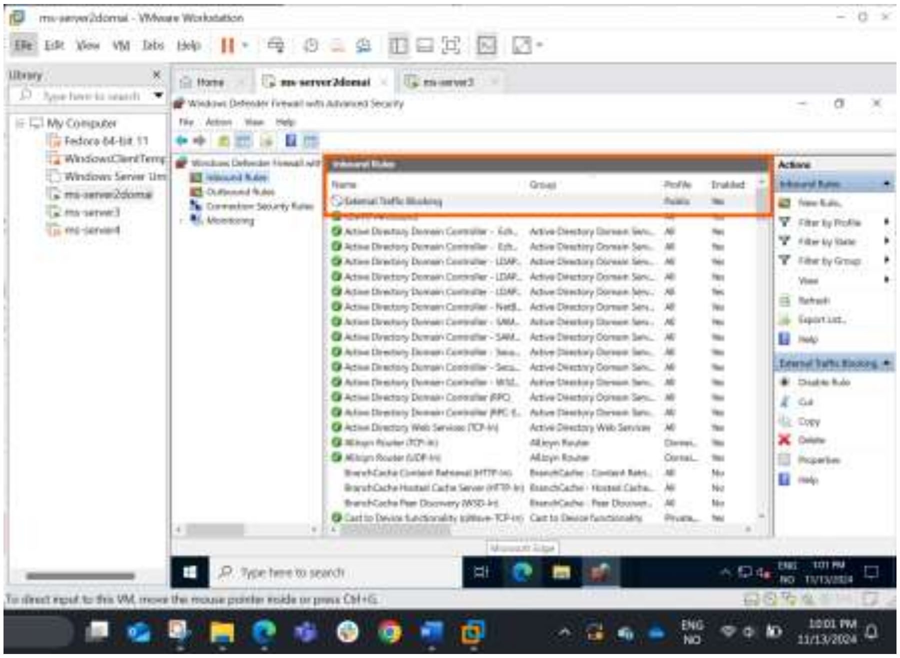
Security and protection of the customer's data is at the forefront of their policy and the best way to protect the data is by encrypting data when it is at 'rest' and 'in transit'. Encryption protects data by transforming the data into unreadable text until data reaches authorized users. Only authorized users can decrypt the data using their decryption key. So, even if hackers get their hands of encrypted (sensitive) data, they will not be able to access the data without this decryption key. The other important encryption feature is Encrypting File System (EFS) that encrypts particular files or folders. This makes it easier to add an extra layer of protection to sensitive files and safeguard confidential data. Internet Protocol Security (IPsec) is another feature that encrypts data when it is on the 'move' across companies' network (between server and devices) (Microsoft, n.d.). For example, it is possible to configure it via Windows Firewall to make sure that data traveling inside the company's internal network stays confidential until it reaches the intended authorized user. In conclusion, encryption is the best 'plan B' security strategy, where in case of security breach, unauthorized user will not be able to use the data. This is 'must have' solution for Cloudy Nerds and High Clouds because they work with sensitive data.

Firewall

Firewall is an essential tool when it comes to network and server security. Firewall regulates users trying to access the network and grants entry only to those users who are authorized to enter. It blocks all traffic unless they are specifically given access to the network by using rules that can grant specific access to applications and ports. For instance, we can create a rule to block specific ports such as internet port - port 80 (or 443). Firewall protects against malware by blocking programs that behave suspiciously. For example, Windows Defender Firewall with Advanced security can protect On-premises system by protecting sensitive areas, establishing security zones, and using rules. In the case of customer with different locations, internal/external networks and different departments, it requires protection for each layer and security zone. It can keep sensitive data safe by creating security zones inside the internal network and blocking unknown connections from the internet as well as other department users. For instance, these sensitive zones can be created for the Finance department, where all traffic coming from external sources and other departments will be blocked. This multi-layer protection approach is golden standard and essential tool to protect the data even if the first layers of the defense are compromised.

The other important use of the firewall is demilitarized zones, where the company can create separate isolated safe environments for internet facing servers that help run the website. The company's sales department runs a website for marketing and product promotion purposes which is customer facing. This webpage server will need to be in its own demilitarized zones that separate it from the internal servers where other company-related data might reside. This separation of public facing server will minimize the hacker's ability to reach the internal network or sensitive zones which we talked about earlier. In conclusion, firewalls are an essential component of the security to protect the customer's network, sensitive data and unauthorized access.

See below the snip for inbound rule wizard for Defender Firewall:



Inbound Rules

Name	Group	Profile	Enabled
External Traffic Blocking		Public	Yes
Active Directory Domain Controller - Ech...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - Ech...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - NetB...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - SAM...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - SAM...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - Secu...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - Secu...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller - W32...	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller (RPC)	Active Directory Domain Serv...	All	Yes
Active Directory Domain Controller (RPC-E...	Active Directory Domain Serv...	All	Yes
Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retri...	All	No
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discover...	All	No
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private...	Yes

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Certificate Authority

An important component in a Windows environment for having secure communication and authentication in an organization is a Certificate Authority (CA). This is achieved by issuing digital certificates that verify the identity of the users, devices and services while encrypting data transmission, keeping it safe from unauthorized access. For example, it can be used for internal communication where offices are in different locations and still have a trusted network that will keep access safe. Even when accessing sensitive documents remotely, authentication of the login credentials is going through encrypted channels. Furthermore, establishing SSL/TLS certificates, internal web pages get secured and ensure secure transmission of the documentation.

By having your own CA, company keeps full control over the certificates and avoid being dependent on others. This is beneficial for keeping secure and still manage hybrid infrastructure that provides remote work possibilities. Additionally, auto enrollment policy provides the possibility for any device that connects to the network automatically and gets necessary certificates by improving security and lowering administrative tasks. To summarize, CA implements secure communication via digital certification that verifies the login credentials, encrypt data, and enables trusted internal communications.

Security and other best practices: Here is simple advice to implement for the customer.

- **Admin Hardware**: Create separate an administrative account, separate laptop and give strong password. Sys Admin should have one laptop only for network management and the other one for everything else.

- **VPN** access is better to administrate the server for secure remote access instead of RDP using an external internet connection.

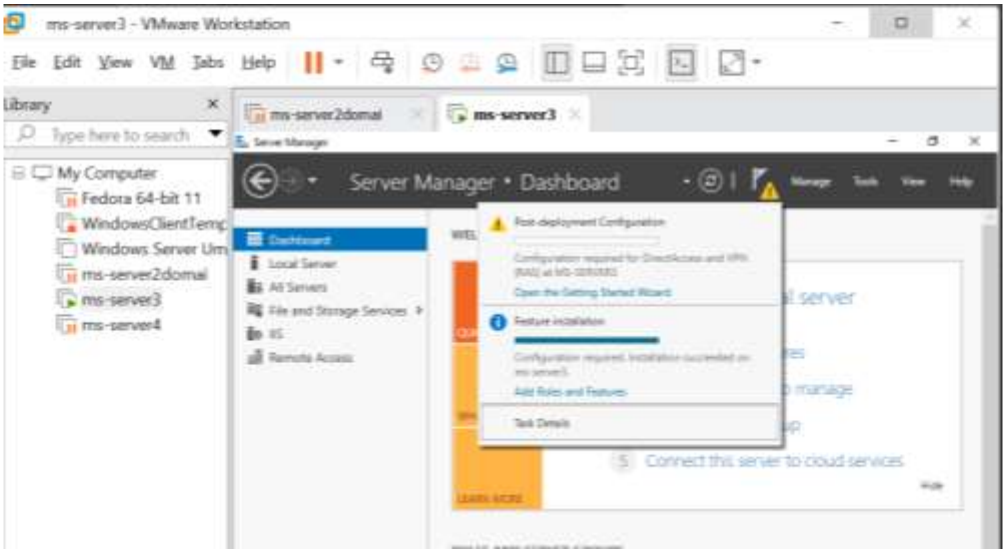
- **AOVPN**: Always On VPN (AOVPN) creates a tunnel that serves as an isolated highway between user and company network. AOVPN is an upgraded VPN tool which automatically detects when linked client device is outside company’s network and automatically turns on the VPN tunnel, not leaving a change for hackers to attack unprotected device (NIST, 2016).

Remote access

Remote Access Management in Windows Server is a tool that allows the administrator to operate servers and network from any location. Usually, it is advised for administrator to control that server inside the internal network and work directly withing the console due to safety, but thanks to remote access technology it is possible to safely access servers without compromising on the security. This tool is in high demand due to growing demand in remote working environments. Similarly, merging companies in two different locations and Management, Consultants and Sales employees need to be able to perform their job and access network anywhere in the world. Remote access is a tool that combines DirectAccess, VPN, and Web Application Proxy in a single console (Microsoft, n.d.).

DirectAccess allows a secure remote connection between company network and domain devices and allows administrators to manage those devices remotely. Direct access establishes securely own tunnel protected by IPsec and automatically detects if the device is in the corporate network or connecting remotely. The automatic establishment of secure tunnels is an important part that makes it a useful tool. It takes away the responsibility of the user to turn on the VPN every time they are logged-in remotely and it allows network administrator to remotely regulate the devices. It means that it performs all necessary actions to establish secure connections, consequently reducing the risk of exposing the corporate network to external attacks (Noroff, n.d.).

See Remote Access Configuration



Post-deployment Configuration

Configuration required for DirectAccess and VPN (RAS) at MS-SERVER3

Open the Getting Started Wizard

Feature installation

Configuration required. Installation succeeded on ms-server3.

Add Roles and Features

Task Details

2.2 Moving to Cloud

The second half of the report will include these cloud infrastructure technologies: benefit of moving to cloud, costs, features like scalability and availability, security, migration phases, proof of work, Azure TCO Calculator analyses etc. It is advised to the Cloudy Nerds and High Clouds to move some of their workload to Azure mainly because of scalability and cost efficiency, while keeping the sensitive and critical workloads in their On-Premises.

2.2.1 Benefits of moving to Azure: Feature

CapEx vs OpEx

On of the biggest significance of moving to cloud from On-Premises is based on cost management. In Capital Expenditures (CapEx), companies need upfront investment to buy and maintain their On-Premises hardware. In Operational Expenditures (OpEx) customer rent the compute and storage resources they need from cloud providers (like MS) and pay for only resources they used. Because of this virtualization, customers significantly reduce the cost on manual hardware maintenance and avoid running idol servers. It is advised Cloudy Nerds and High Clouds to utilize the pay-as-you-go pricing model because it will help to reduce hardware and other operating costs, while quickly adjusting to volatile business needs.

In the case of Cloudy Nerds and High Clouds, they have developers team and create and test application for their customers which require volatile usage of resources for a short period of time. So, instead of creating and maintaining On-Premises resource that can handle testing the application and remain idol the rest of the time, it is cost effective for the customer to move that workload to Azure and use Azure DevTest Labs for scalable testing environment for development. It will allow the customer to scale up for web test and reduce/delete the resource once they are done. This will allow dynamic scaling and provide optimal utilization without overprovisioning.

Now, moving to the OpEx model does not mean that Cloud provider like Microsoft (MS) will automatically be responsible for handling everything, it simply means that these responsibilities are shared between the cloud provider and customer. The Shared responsibility is connected to cloud services types of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Infrastructure as a Service (IaaS) has the least virtualization where MS is only responsible for physical security, internet connectivity, and power of data centers. This means that a customer will be responsible for everything else, just as they would in the On-Prem. The opposite side of the spectrum is SaaS, where MS is responsible for virtualization of application, network control, OS, physical security, network and datacenter maintenance. While PaaS is somewhere in between IaaS and SaaS, where identity and directory infrastructure, applications and network control are shared between cloud providers and customer.

Scalability

Scalability is the important advantages of moving to cloud because it allows adjusting resource dynamically to meet the high or low demand. There are two types of scalabilities: vertical scaling which increases and decreases the capacity of a server (CPU and RAM in a VM), while horizontal scaling is about adding additional server or VM to the system for additional support and distribution. Horizontal scaling is ideal for environments with that need to handle large demand for a short period of time and when the demand subsides, they can reduce/delete the resource. Considering the fact that just testing web applications requires volatile demand of resources, scalability of cloud resources will be immensely beneficial for developers departments. Azure DevTest Labs can streamline developers workflow, enhance the reliability of applications and decrease the risk of error in their production phase. The workload needs adjustability for test environment and facilitate low costs while providing all the required tools for developers to do their jobs. Moving their workload to Azure, particularly to Azure DevTest Labs will not only resolve their scalability challenge, but also provide isolation, and cost control.

High Availability:

The other benefits of using cloud services are high availability that focuses on providing the maximum availability without disruption and data loss. When an IT company builds and deploys application as part of their service, they need to make sure that their services are available (almost) all the time and preferably without disruption. The only way to solve that is either build a resilient data center that will be very costly for small companies or alternatively use a public cloud provider that guarantees high availability under their Service-Level Agreement (SLA). The uptime guarantee through their SLAs is around the range of 99% to 99.99%. This high availability is great for the customers who have public facing retail website and host it in Azure Apps Services, for example, which provides 99.9% uptime SLA.

Accessibility – Collaboration

Accessibility is another advantage for customer to migrate some of their workload to Azure due to seamless collaboration and workflow without compromising on security and giving guest access to their internal network. For example, hosting the DFS system in Azure Files will provide the consultants, sales staff, and design teams with the right access to the critical files from anywhere in the world. Azure's Role-Based Access Control (RBAC) is a tool that helps to ensure the right permission is given to the right user/role. In On-Premises network, network administrator uses VLAN, AD, Active Directory Rights Management Services (AD RMS), Dynamic Access Control (DAC), etc. to compartmentalize, isolate network and control the access of critical files to the 'right' users/roles, while in Azure it is mainly RBAC job to control the permission to the right user/role. In this particular case, if the DFC system is to move to Azure, cloud administrator could utilize RBAC and give full control to consultant, the Write access to design team to configure the files, while sales team would get Read-only access. This tool simplifies access management while at same time increasing productivity by reducing potential delay caused by access requests.

Another good use-case for accessibility and collaboration is File Server for **Guest Accounts**. It was mentioned in the services requirements given by Cloudy Nerds and High Clouds that they need to collaborate with their customer to showcase and assess the web product. In order to get feedback on the product they build for their customers, Cloudy Nerds and High Clouds need to give guest access to their customer without compromising security for the rest of their workload. So, File Server for Guest Accounts would allow guess user to get Read-only access for a short amount of time to see the isolated cloud environment, while not allowing external users to access to internal network. This combination would result the better collaboration with their customer without compromising their internal network.

Cloud Security

When it comes to security, Azure (together with other public cloud providers) have a state-of the art security system in place that can mimic the On-Premises network solutions we have discussed in the first half of the report. Azure has a range of security tools to choose from that can be tailored to the customer's need, however it is important to keep in mind that public clouds cannot provide 100 percent ownership of the data, flexibility, tailored data modeling or distribution and compliance of data according to local regulations that is it, customer is advised to keep sensitive data on Premises for compliance purposes even if the is not cost effective. And the rest of the cost workload can be moved to Azure to utilize the technology capabilities and lowers costs. Cloudy Nerds and High Clouds can make sure the 'right' access is given to the resources by using the Azure Active Directory, which can be seamlessly integrated into the On-Prem's Active Directory. This means that the same user can have access to the environment if there is a need without creating a new account.

2.2.2 Benefits of moving to Azure: Cost

According to the Azure's Total Cost of Ownership (TCO) Calculator, it is predicted yearly saving cost of hosting key workloads with the DFS system measure to 27,209,049 kroners, and developer test environment savings goes up to 199,187,778 kroners (details shown below). All of this comprises of the storage, compute resources, and content delivery services. In comparison to maintaining the similar on-premises infrastructure, it shows major saving in operational costs as well as giving extra flexibility and scalability.

Proof of Work

A comprehensive example is provided by the Azure Total Cost of Ownership (TCO) Calculator when comparing on-premises infrastructure costs versus cloud adoption costs. The cost analysis shows and tells more to decision making and displays the value of cloud migration. The TCO Calculator would assess expenses connected with maintaining on-premises infrastructure for services like the DFS system, and developer test environments that we are advising customer to move to cloud. Operational cost would be included such as hardware purchases, electricity, cooling, IT labor for maintenance, and software licensing. All of this would be than compared to Azure's cloud-based services, which operate on a pay-as-you-go model.

Azure TCO Calculator

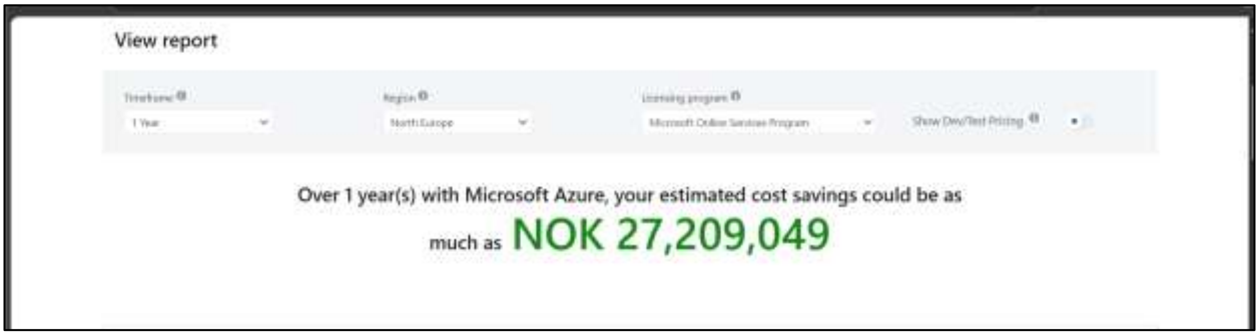
For on-premises infrastructure, there are significant upfront costs for purchasing and maintaining physical servers, storage devices, and networking equipment. Azure eliminates these capital expenditures, replacing them with operational costs that scale dynamically with actual usage. This is particularly advantageous for startups like Cloudy Nerds and High Clouds, where budget flexibility and cost efficiency are critical.

DFS System workload in TCO Calculator

Azure TCO calculator offers approximate prediction for expenses to run the same workload in Cloud and On-Premises, but it is important to keep in mind that it is giving estimate among and may change in real scenario. For DFS System workload, we will estimate using Azure Files with 2 servers, 8 processor cores, 16 GB RAM per server, and 500 GB of storage etc. This input calculated approximately 27,209,049 kroners cost saving (annually) if the same workload would be moved to Azure instead of running to On-Premises.

These calculations show that it is much cheaper for customer to move their DFS systems to cloud storage systems for at least the non-sensitive data that can drastically reduce the cost and administrative overhead without give out lacking for feature shortcomings.

See the snip below for the results DFS system in TCO:



View report

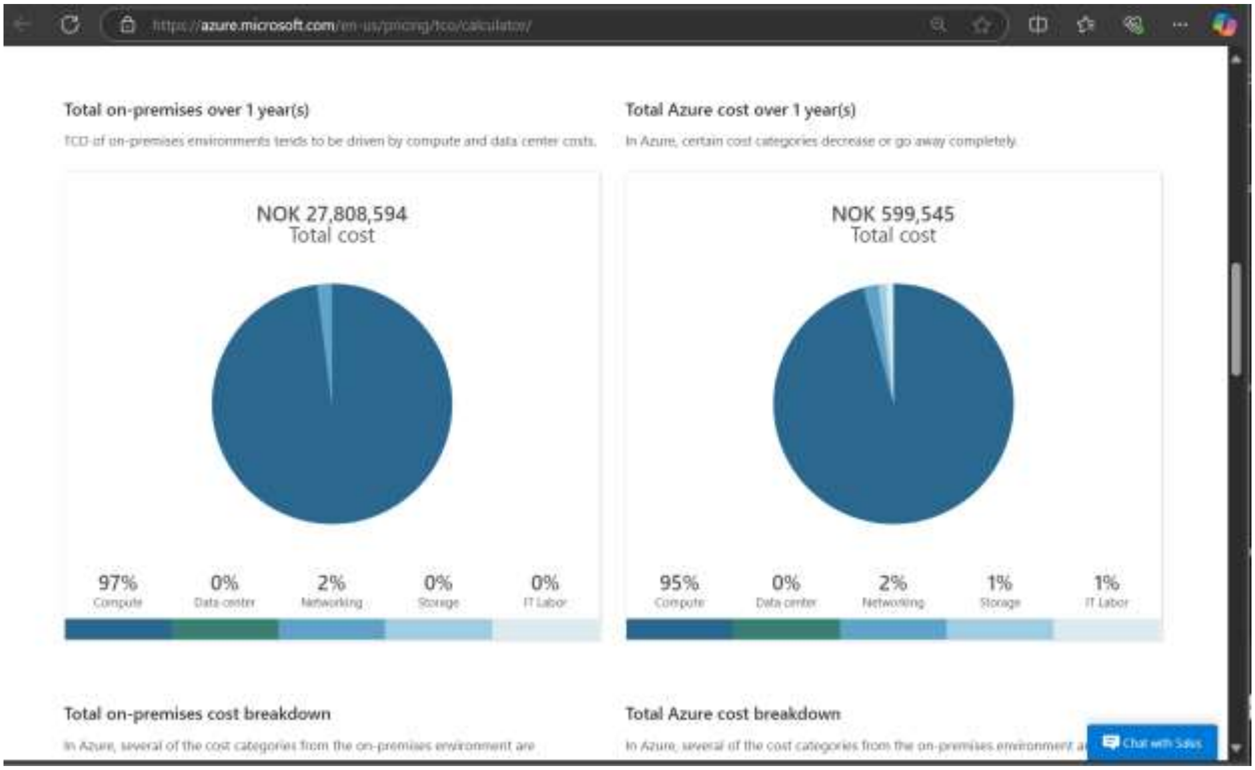
Timeframe: 1 Year

Region: North Europe

Licensing program: Microsoft Online Services Program

Show Dev/Test Pricing

Over 1 year(s) with Microsoft Azure, your estimated cost savings could be as much as NOK 27,209,049



Total on-premises over 1 year(s)

TCO of on-premises environments tends to be driven by compute and data center costs.

NOK 27,808,594
Total cost

Total Azure cost over 1 year(s)

In Azure, certain cost categories decrease or go away completely.

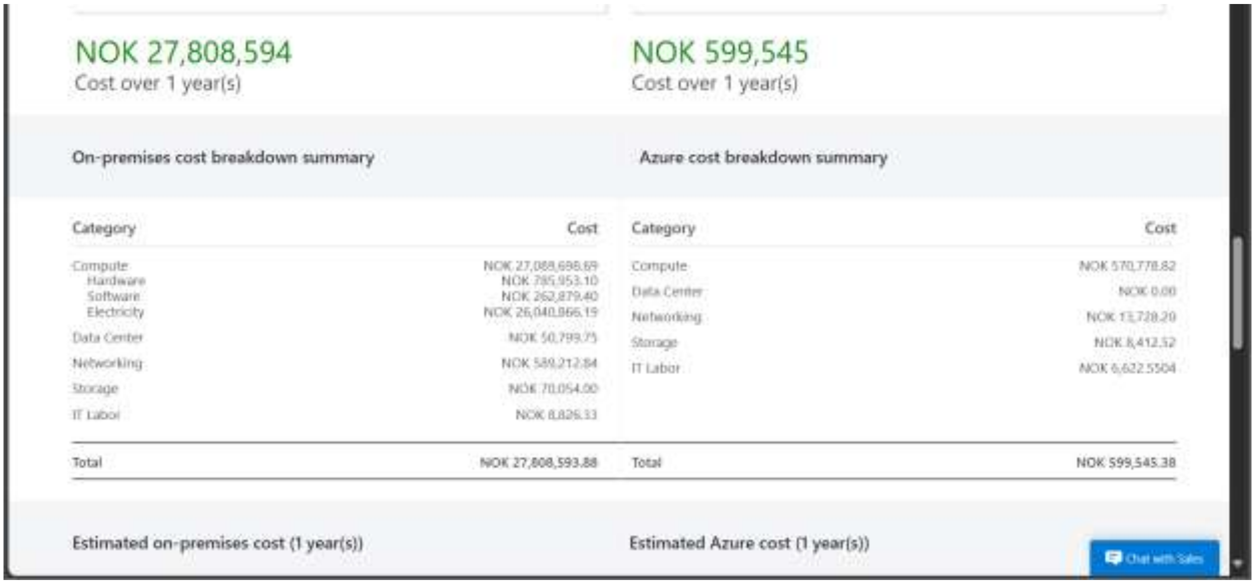
NOK 599,545
Total cost

Total on-premises cost breakdown

In Azure, several of the cost categories from the on-premises environment are

Total Azure cost breakdown

In Azure, several of the cost categories from the on-premises environment a



NOK 27,808,594
Cost over 1 year(s)

NOK 599,545
Cost over 1 year(s)

On-premises cost breakdown summary

Category	Cost
Compute	NOK 27,088,698.69
Hardware	NOK 785,953.10
Software	NOK 262,879.40
Electricity	NOK 26,040,866.19
Data Center	NOK 50,799.75
Networking	NOK 589,212.84
Storage	NOK 70,054.00
IT Labor	NOK 8,826.33
Total	NOK 27,808,593.88

Azure cost breakdown summary

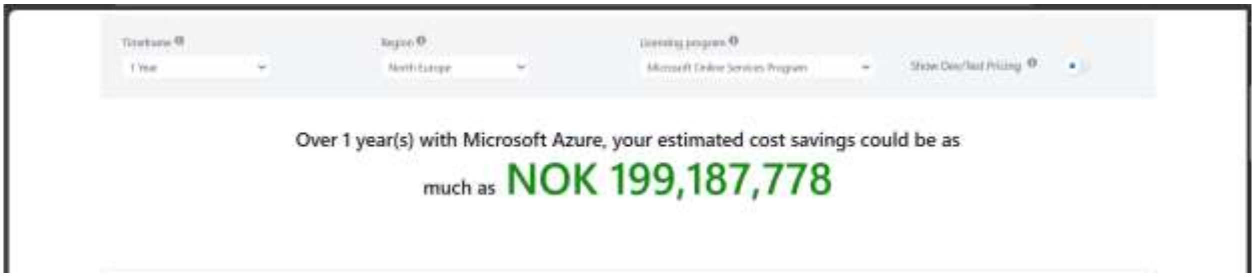
Category	Cost
Compute	NOK 570,778.82
Data Center	NOK 0.00
Networking	NOK 13,728.20
Storage	NOK 8,412.52
IT Labor	NOK 6,622.5504
Total	NOK 599,545.38

Estimated on-premises cost (1 year(s))

Estimated Azure cost (1 year(s))

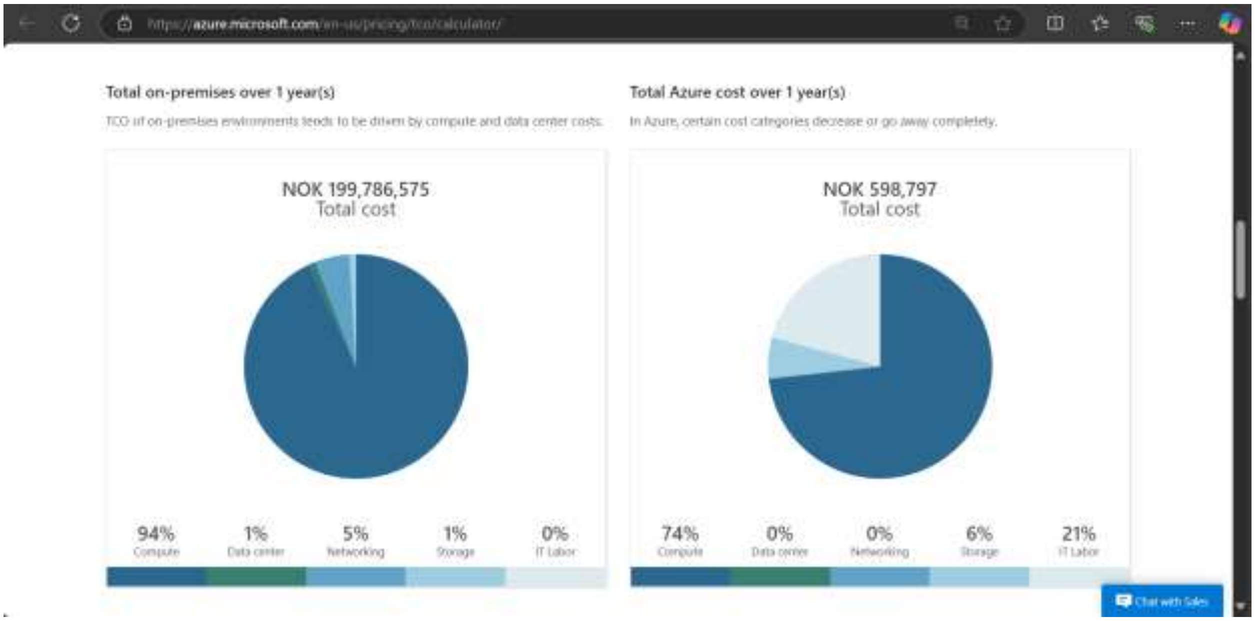
Developer environment workload in TCO Calculator

The other workload that we have to advise the Cloudy Nerds and High Clouds to move to Azure is Developer environment. Here are some estimates we have put into TCO calculator to get estimated cost saving amount are: use Azure DevTest Labs with 5 servers, 4 processor cores per each server, 32 GB RAM per server, SSD disk, 2 TB main storage, and of Azure 4 TB backup storage etc., which resulted to approximately 199,187,778 kroners saving cost per year if the same workload would be moved to Azure instead of running to On-Premises. See snip below for the results Developer environment in TCO:



Timeframe: 1 Year
Region: North Europe
Licensing program: Microsoft Online Services Program
Show Dev/Test Pricing

Over 1 year(s) with Microsoft Azure, your estimated cost savings could be as much as NOK 199,187,778



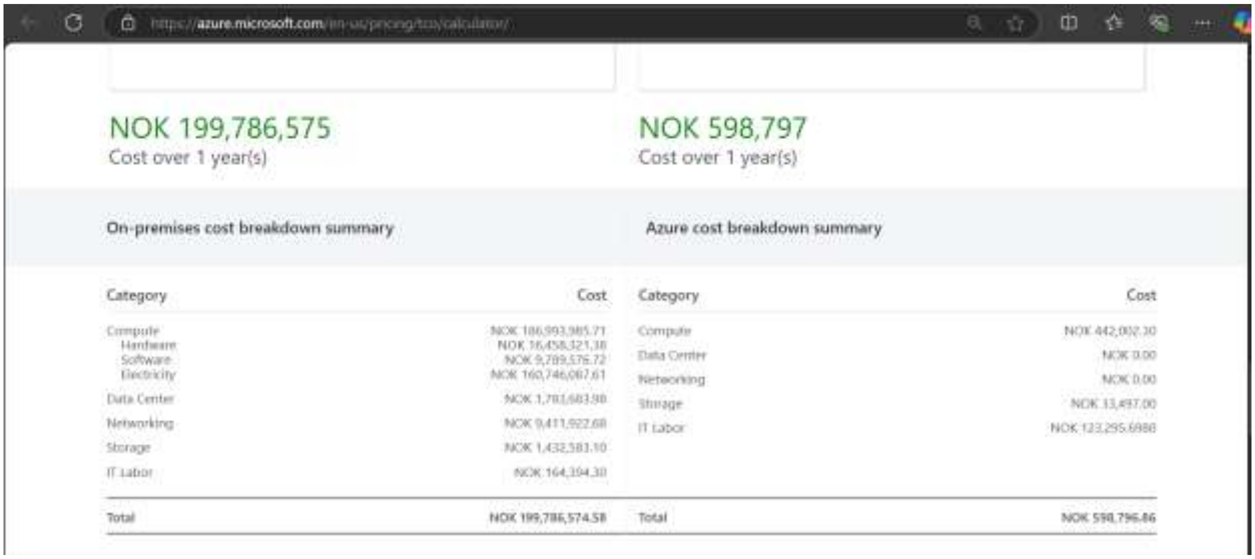
https://azure.microsoft.com/en-us/pricing/tco/calculator/

Total on-premises over 1 year(s)

TCO of on-premises environments tends to be driven by compute and data center costs.

Total Azure cost over 1 year(s)

In Azure, certain cost categories decrease or go away completely.



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

NOK 199,786,575
Cost over 1 year(s)

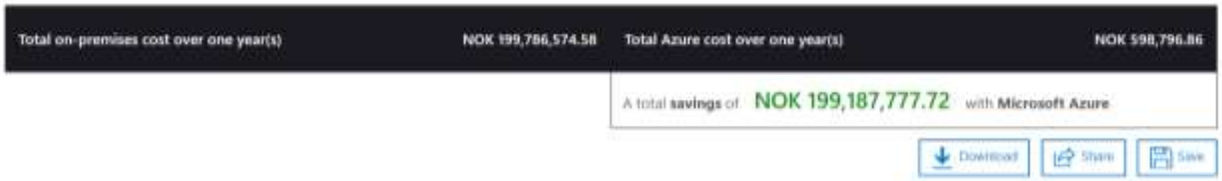
NOK 598,797
Cost over 1 year(s)

On-premises cost breakdown summary

Category	Cost
Compute	NOK 186,993,985.71
Hardware	NOK 16,458,321.38
Software	NOK 9,789,576.72
Electricity	NOK 160,746,087.61
Data Center	NOK 1,783,683.98
Networking	NOK 9,411,922.68
Storage	NOK 1,432,383.10
IT Labor	NOK 164,394.30
Total	NOK 199,786,574.58

Azure cost breakdown summary

Category	Cost
Compute	NOK 442,002.30
Data Center	NOK 0.00
Networking	NOK 0.00
Storage	NOK 33,497.00
IT Labor	NOK 123,295.6988
Total	NOK 598,796.86



Total on-premises cost over one year(s)	NOK 199,786,574.58	Total Azure cost over one year(s)	NOK 598,796.86

A total **savings** of NOK 199,187,777.72 with **Microsoft Azure**

This diagram clearly shows that migrating the developers environment to Azure can provide significant cost having for customer and provide them with detailed cost overview of the tools. This tool is great to give an overview and provide predictive analysis for estimated future usage of Azure resources which could be highly useful for customer to allocate the budget for cloud resources. It Azure Cost Management also has features like tagging resources for cost allocation, setting budgets, real-time alerts for overspending and making sure that customers (resource) do not overspend.

The TCO Calculator provides a breakdown of expenditures that can be used by stakeholders and provides them with financial information that further affects their decision and ensures that they align with their business goals. The cloud's operational cost model gives opportunity to increase or decrease resources depending on the workload demands. For instance, when product is being launched developers can increase test environment, and during downtime it can be decreased which would help with skipping needless cost. Financial risk connected with unexpected market changes has decreased due to the minimal upfront investments. This is of great help for startups who are usually with insecure income streams.

Moving to cloud might have some initial adjustment to the employees and environment but the long-term benefits clearly outweigh these inconveniences. TCO calculator has clearly shown the cost benefits, and we have discussed other technical features like scalability, availability, collaboration, and security that could also be beneficial for the customer. For Cloudy Nerds and High Clouds, this analysis not only justifies the investment in Azure but also underscores the strategic alignment of their IT infrastructure with business growth objectives. The hybrid approach provides the possibility to keep control over sensitive and highly confidential systems in On-Prem, while at the same time leveraging the cloud for scalable and solutions available across the world. Having Azure's advanced tools and best practices, anyone would put themselves in a situation of sustained growth and innovation.

3. <u>Summary</u>

In conclusion, this report provides a recommendation for merging Cloudy Nerds and High Clouds as well as an evaluation for potential move. It is advised to Cloudy Nerds and High Clouds to establish a hybrid infrastructure, where most of the workloads are based in the On-Premises environment due to the importance of data ownership, security and compliance, while migrating some workloads to Clouds due to flexibility, scalability, high availability and cost-effectiveness of the Cloud infrastructure.

This approach ensures critical workloads requiring strict security and compliance remain On-Premises, while leveraging flexible, limitless, and (relatively) cheap services in Azure. By retaining sensitive data locally and migrating services like the DFS system and developer environments to Azure, the merged company achieves a balance between security, cost savings, and agility. Azure's tools like DevTest Labs and RBAC enhance collaboration and efficiency, while on-premises systems maintain full control over sensitive resources. This hybrid model offers the best of both worlds, supporting the company's operational needs and long-term growth. Based in this report it is safe to conclude that Cloudy Nerds and High Clouds should first focus on merging and strengthening their On-Prem infrastructure since most of their workload is based on, but if the leadership team wants to crease their business and income, they should definitely consider virtualizing hardware maintenance and move their workloads (like DFS/developers) to Azure.

4. References

Comer, D. E. (2018). *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (6th ed.). Pearson.

Kinsta. (n.d.). *What is FTP?* Retrieved from https://kinsta.com/knowledgebase/what-is-ftp/

Krause, J. (2021). *Mastering Windows Server 2019.* Packt Publishing.

Microsoft Learn (2024). *Microsoft Certified: Azure Fundamentals - Certifications.* Available at: https://learn.microsoft.com/en-us/credentials/certifications/azure-fundamentals/?practice-assessment-type=certification.

Microsoft Learn. Exam AZ-900: Microsoft Azure Fundamentals - Certifications | Microsoft Learn

Microsoft. (n.d.). *Azure Active Directory Connect and hybrid identity*. Microsoft Learn. Retrieved December 6, 2024, from https://learn.microsoft.com/en-us/azure/active-directory/hybrid/

Microsoft. (n.d.). *Azure Virtual Desktop documentation*. From https://learn.microsoft.com/en-us/azure/virtual-desktop/

Microsoft. (n.d.). *Azure Virtual Desktop workloads*. From https://learn.microsoft.com/en-us/azure/well-architected/azure-virtual-desktop/

Microsoft. (n.d.). *Azure VPN Gateway overview*. From https://azure.microsoft.com/en-us/products/vpn-gateway/

Microsoft. (n.d.). *Azure VPN Gateway topologies and design*. From https://learn.microsoft.com/en-us/azure/vpn-gateway/design

Microsoft. (n.d.). *Certificate Services Overview*. Retrieved from https://learn.microsoft.com/en-us/windows-server/identity/ad-certificate-services/

Microsoft. (n.d.). *Distributed File System Namespaces*. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/dfs-namespaces/dfs-overview

Microsoft. (n.d.). *Overview of DFS Replication*. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/dfs-replication/dfsr-overview

Microsoft. (n.d.). *Overview of FTP server on Windows*. Retrieved from https://learn.microsoft.com/en-us/iis/publish/using-the-ftp-service/overview-of-ftp

Microsoft. (n.d.). *Overview of Windows File Server and file sharing*. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/file-server/

Microsoft. (n.d.). *Storage Replica overview*. Retrieved from https://learn.microsoft.com/en-us/windows-server/storage/storage-replica/storage-replica-overview

Microsoft. (n.d.). *Work remotely with VPN Gateway*. From https://learn.microsoft.com/en-us/azure/vpn-gateway/work-remotely-support

YouTube Video 2: TechAcademy. (2022, April 15). Access Control List (ACL) Basics Explained [Video]. From YouTube. https://www.youtube.com/watch?v=kfvJ8QVJscc&t=151s