



Proposal for PromisedLand at Hukilau Marketplace

BY DAVID ODEDIRAN

2022

PromisedLand

Tel +233545666550
Fax +233549012520

55-370 Kamehameha Hwy, Laie, HI.
96762

PL.com
admin@pl.com

Table of Contents

Introduction to PromisedLand Server Architecture _____	1
Brief Summary _____	1
Organization Chart _____	1
Server Architecture and Server Baseline _____	3
Server architecture _____	3
Server Baseline _____	4
Storage Capacity _____	5
Hardware and Software Troubleshooting _____	8
Server Backup/Restore _____	11
Users and Groups for Active Directory _____	14
Principle of Least Privilege (POLP) _____	17
Encrypted File System _____	20
Users who can access the encrypted file _____	21
Security Protection _____	22
Network Security _____	22
Firewall rule and allow Remote Desktop Protocol User Mode _____	22
Access Control List and Why PromisedLand Should use it _____	23
Network Intrusion Detection System _____	23
Lightweight Directory Access Protocol (LDAP) _____	24
Encrypting the Communications in PL.com _____	24
Two Reasons why VPN are useful to PL.com _____	25
How VLAN secure data on a network _____	25
Physical Security Methods and Concepts _____	26
PromisedLand implementing the use of a mantrap in their data centers _____	26
1. Closed-circuit television (CCTV) camera surveillance _____	27
2. Uninterruptible power supply (UPS) _____	28
3. Cooling System _____	28
Implementing an additional multi-factor authentication on my personal accounts _____	28
Server Hardening _____	30

Table of Contents

Disadvantages of computer security configuration _____	30
Implication of Services on computer security _____	31
Ports in use by programs on the Windows Server _____	32
Using Tasklist command _____	33
Using Netstat command _____	33
Anti-malware software is installed by default on a Windows Server? _____	33
Disaster Recovery _____	35
HIGH-LEVEL OUTLINE OF DISASTER RECOVERY PLAN _____	35
KEY PERSONNEL AND CONTACT INFORMATION _____	36
INFORMATION SERVICES BACKUP PROCEDURES _____	37
DISASTER RECOVERY PROCEDURES _____	37
RECOVERY PLAN FOR COLD SITE _____	38
RECOVERY PLAN FOR HOT SITE _____	38
RESTORATION PROCESS _____	38
RECOVERY PLAN PRACTICE AND EXERCISING _____	38
DISASTER SITE REBUILDING _____	39
PLAN CHANGES OR UPDATES _____	39
Cost of Recommended Servers for small businesses _____	40
Dell. PowerEdge T30 _____	40
Dell. PowerEdge T20 [barebones] _____	41
Lenovo. ThinkServer TS150. _____	42
HPE. ProLiant ML350 Gen 10 _____	43
Fujitsu. Primergy TX1310 M1 _____	43
HP. ProLiant Microserver Gen8 _____	43
Lenovo. ThinkServer TS460 _____	44
HP. ProLiant ML350 G9 5U _____	45
Project Implementation Approval _____	46
Project summary and approval _____	46
Contact Information _____	47
School Details _____	47

Table of Contents

“Be courageous. Challenge orthodoxy. Stand up for what you believe in. When you are in your rocking chair talking to your grandchildren many years from now, be sure you have a good story to tell.”

— Amal Clooney

Introduction to PromisedLand Server Architecture

Brief Summary

The location at the Hukilau Marketplace at 55-370 Kamehameha Hwy, Laie, HI. 96762 is a perfect spot for tourist business. Leveraging an IT integrated environment ensures the success of the business as computers managed business guarantees a high success rate. They also allow communication between larger hotel chains with multiple locations to connect easily. Moreover, they also help keep staff on the same page and make it easier to access information, making our guest's experience much better. As we all know, a technology-integrated environment helps reduce costs, enhance operational efficiency, and improve services and customer experience. From the look of things, the office space will accommodate 45 employees and would be managed based on the organization charts provided (see [Figure 1.1](#)). The office would serve as a hybrid call center that includes the following units: tourist guide, which assists, information on culture, historical and contemporary heritage to people looking for guided sightseeing tours.

Organization Chart

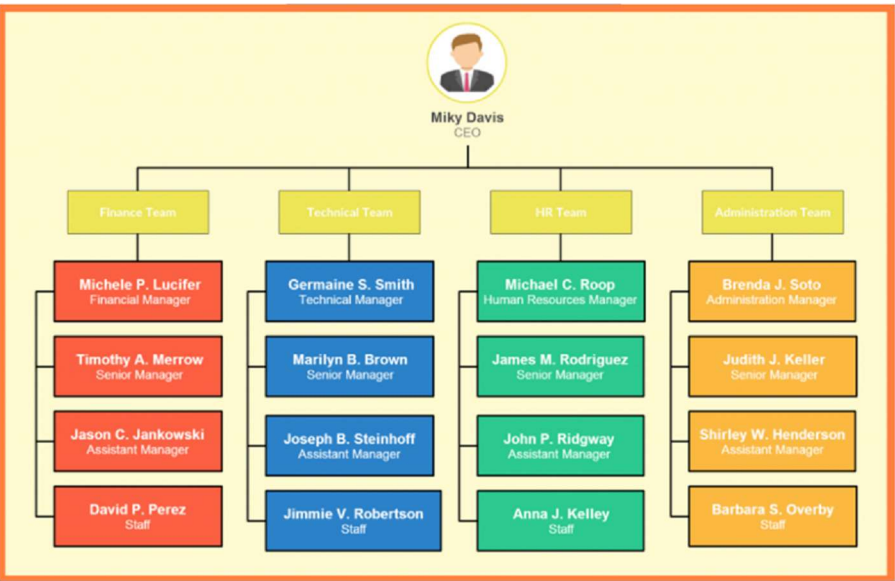


Figure 1.1

This executive summary addresses basic server implementation about full office deployment of PL.com domain and how PromisedLand stands the chance of benefiting from server integrated into the company's operational activity. The executive summary for this project includes an embedded video presentation of my proposal for full office deployment of PL.com. This project demonstrates my ability to:

- Install, configure, manage, and maintain a server.
- Implement and support disaster recovery solutions, backup techniques, and storage device technologies.
- Apply physical and network data security techniques.
- Troubleshoot network connectivity, systems hardware, software, connectivity storage, and security issues.

At the end of the whole exercise, you will see how each part of the organization elements will be integrated into full office deployment. The record of a newly configured server using the documents as a reference point to the official deployment of the PromisedLand server, which is installed on a virtual machine for explanation and experimental purposes. The recorded activities of the exercise are attached with the documents for clarity.

David Odediran



March 26, 2022

Server Architecture and Server Baseline

Server architecture

Server architecture is the foundational layout or model based on which a server is created and deployed. It defines how a server is designed and the different components created from its services. Server architecture primarily helps design and evaluate the server and its associated operations and services before deployment. Server architecture includes, but is not limited to:

- The physical capacity of a server (computing power and storage)
- Installed components
- Types and layers of applications and operating system
- Authentication and overall security mechanism
- Networking and other communication interfaces with other applications and services

I will be providing a new installation for the company using the following settings:

- Type of configuration: Typical
- Using my ISO file for Windows Server 2019 Datacenter
- Guest Operating System selection - Microsoft Windows/Windows Server 2016
- Virtual Machine Name: My Name - IT 235 using the default file location
- Maximum disk size (GB): 60
- Store virtual disk as a single file (see Storage Capacity)

I will also be putting in place some settings for effective deployment and walkover for usability and clarity. These settings and configuration include;

- I set up the new virtual machine using the above settings, rename the Administrator account to FriendlyFace.
- Generate a 16-character password to the FriendlyFace administrator account.
- To manage PromisedLand's devices connected to the network,
 - Set a 13-character minimum password for the Administrator account.

- Assign an IP address to the network interface card or continue to use DHCP. (The best practice is to assign a static IP address for each server).
- The Root Domain in the new forest will be labeled PL.com.
- Install the following server roles
 - ADDS
 - DNS
 - DHCP

Server Baseline

A baseline is an ideal or standard configuration for that node. It is the configuration against which user want to judge that node in the future. The server baseline deals with the security measures put in place in the whole deployment. Every organization faces security threats. However, the types of security threats that are of most concern to one organization can be completely different from another organization. For example, an e-commerce company may focus on protecting its Internet-facing web apps, while a hospital may focus on protecting confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must comply with the security standards defined by the organization.

- [Server Backup/Restore](#)
- [Users and Groups for Active Directory](#)
- [Principle of Least Privilege \(POLP\)](#)
- [Encrypted File System](#)
- [Security Protection](#)
- [Server Hardening](#)
- [Disaster Recovery](#)

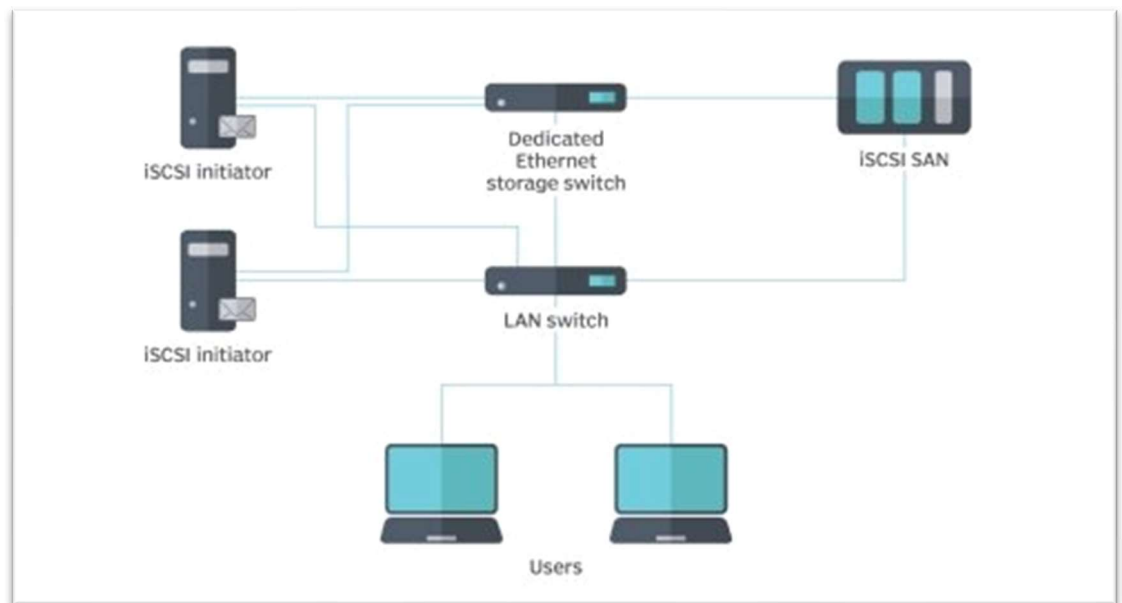
On Server architecture and server baseline, Server architecture primarily helps design and evaluate the server and its associated operations and services before deployment. It also deals with the primary organization of server control flow. The server baseline deals with the security measures in the whole deployment. The one thing that all organizations have in common is a need to keep their apps and devices secure.

Storage Capacity

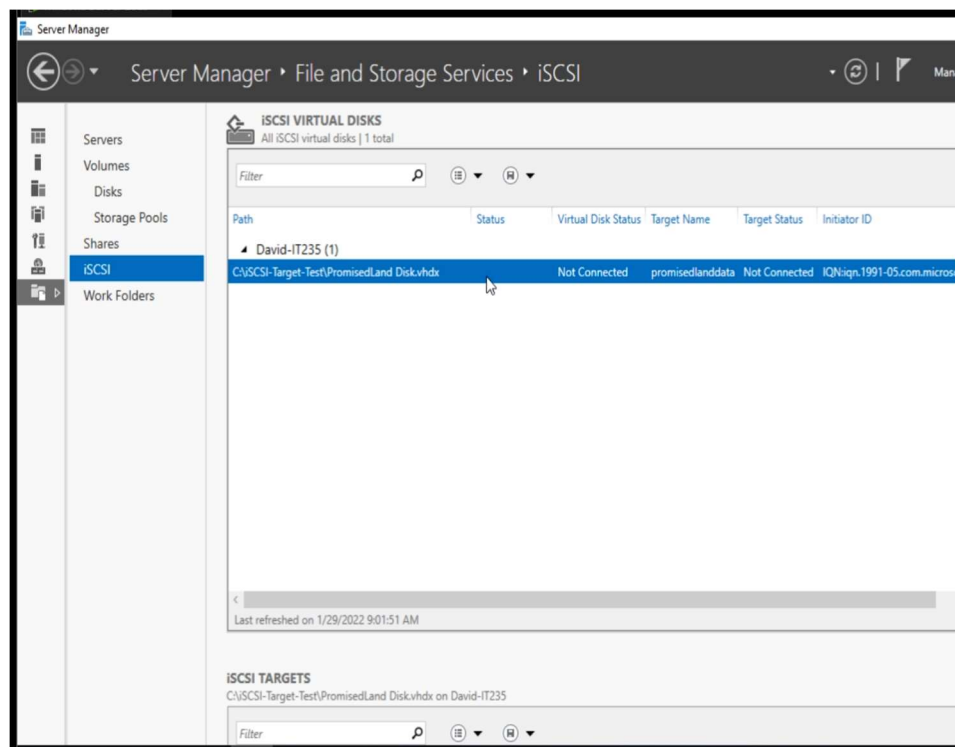
Storage capacity refers to how much disk space one or more storage devices provides. It measures how much data a computer system may contain. For example, a computer with a 500GB hard drive has a storage capacity of 500 gigabytes. A network server with four 1TB drives has a storage capacity of 4 terabytes. For this exercise I make use of a Store virtual disk as a single file with 60 GB capacity.

The major problem most organizations have with storage is the availability of shared documents or resources across the network. One for iSCSI targets was introduced to ensure that resources are shared across the network at a faster rate. iSCSI stands for Internet Small Computer Systems Interface. iSCSI is a transport layer protocol that works on top of the Transport Control Protocol (TCP). It enables block-level SCSI data transport between the iSCSI initiator and the storage target over TCP/IP networks. iSCSI is a block protocol for storage networking and runs the ubiquitous SCSI storage protocol across a network connection, usually Ethernet. iSCSI, like Fiber Channel, can be used to create a Storage Area Network (SAN). iSCSI traffic can be run over a shared or dedicated storage network.

iSCSI server shares resources over the network using the TCP/IP protocol. iSCSI components include; The iSCSI initiator, which is the hardware or software installed on a server to share data. The iSCSI targets the server that hosts the storage resources and allows access to the storage. The iSCSI transport is block-level data between the iSCSI targets and the iSCSI initiator using the TCP/IP internet LAN or WAN. The server creator becomes the target while the members on the network willing to access the resources are the initiator. The essence of iSCSI server storage for PL.com is for employees to access the storage from remote locations.



I will install and configure the iSCSI target on Windows Server 2019. iSCSI an Internet Protocol-based storage networking standard for linking data storage facilities. It provides block-level access to storage devices by carrying SCSI commands over a TCP/IP network. The iSCSI target is the storage on a remote location, which appears to the host system (iSCSI initiator) as a local drive.



The network users of PL.com will be able to access the resources and share data over the network. In this case, the iSCSI server would allow the company workers to share resources across the board. Every organization would like to work by collaboration and sharing resources from one department to another without moving an inch. It's one of the reasons why iSCSI would be of great benefit to the PromisedLand.

Hardware and Software Troubleshooting

Troubleshooting is a systematic approach to problem-solving that is often used to find and correct complex computer system issues. It is also a form of problem-solving to repair the failed computer system. The reason why troubleshooting matters is because it is used in determining the most likely cause is a process of eliminating potential causes of a problem. Finally, troubleshooting requires confirmation that the solution restores the system process to its working state.

Some troubleshooting techniques is as follows;

1. Identifying the problem and determining the scope

It is the first stage of troubleshooting as it provides room for gathering information about the problem and identifying its root cause. The information gathered is used to determine the areas to be addressed in the troubleshooting process.

2. Escalating a theory of probable cause

At this stage, we would be asking what could have caused the problem. The other thing involved would be to check and search through the net for a similar problem and the probable cause when more questions are needed to solve the problem. The other option comes into places, such as Vendor documentation, the organization's documentation, and Google search.

3. Testing the theory to determine the cause

At this stage, If the theory is tested to discover the likely cause and is not successful or incorrect, there is a need for more research to be done all over again.

4. Establishing a troubleshooting plan of action and Implementing solution

At this stage, once the cause has been established, there is a need for an action plan to safeguard the system's current state and keep files and essential documents intact. If the fixes don't work, there is a need to roll

back the machine to the current state before the fixes are implemented or applied.

5. Verifying full system functionality and Implementing Preventative Measures

At this stage, there is a need to verify if fixes have been rectified working correctly and put in place factors that will allow such incidents not to occur again. At this stage, the system is expected to act and respond the way it should work. If not, the whole procedure needs to be re-evaluated.

6. Performing root cause Analysis

The root cause analysis helps to identify the scope of a problem. It is used to trace back these actions. You can discover where the problem started and how it led to it to the present circumstances. Root cause analysis further exposes the individual to likely fixes in this scenario.

7. Documenting findings and actions and outcomes

Documentation is an essential aspect of the whole exercise. It deals with steps, changes, updates, theories, and research that could all be helpful in the future when a similar problem arises (or when the same problem turns out not to have been fixed after all). The primary reason for documentation is that this guide will save a lot of time in implementing this procedure once again if a similar incident occurs.

In summary, Hardware troubleshooting is reviewing, diagnosing, and identifying operational or technical problems within a hardware device or equipment. It aims to resolve physical and logical problems and issues within computing hardware. While Software troubleshooting is the process of scanning, identifying, diagnosing, and resolving problems, errors, and bugs in software. It is a systematic process that aims to filter out, resolve problems, and restore the software to regular operation. There are instances when things don't go according to plan, and at this point, we need to retrace our steps by

using troubleshooting techniques. What do I mean by this? Every law on earth for good deeds has its repercussion. The same goes for evil deeds.

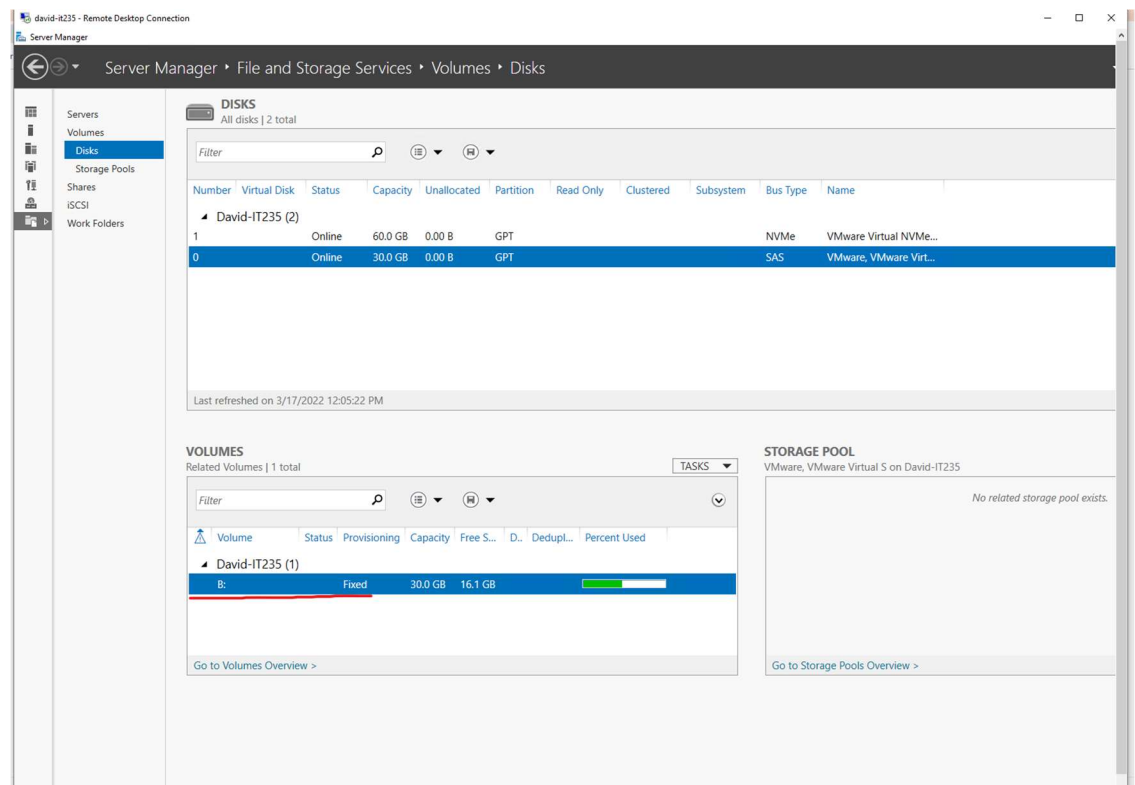
Troubleshooting is a guide that will reshape the way we see problems when they surface.

Server Backup/Restore

Let's say PL.com did not install any backup, and all of a sudden, the system crashed, or some crisis occurred. In what position would the management of PL.com be? It is one of the significant reasons for server backup. Computer backup guarantees a high level of security and peace of mind as it allows data storage off-site/online. It helps you in saving time and costs too. It provides much better protection against natural disasters. Also allows an unlimited amount of data retention. This project aims to install and implement a full server backup of the virtual machine to demonstrate that I can back up the system state data and other vital operating system components.

The Windows Backup process involves creating a backup of the system state data and other vital operating system components at regular intervals. Which is then stored in the system backup at a different place than the original system components, such as a separate system drive, external storage media, or an offsite location. This backup file can help you restore a system or configure a new system to the state at the time the system backup was created. The requirement for this exercise was to create a system backup to showcase how I will do the system backup of the whole operating system components. I was able to do the backup for this aspect of the project by using the following steps;

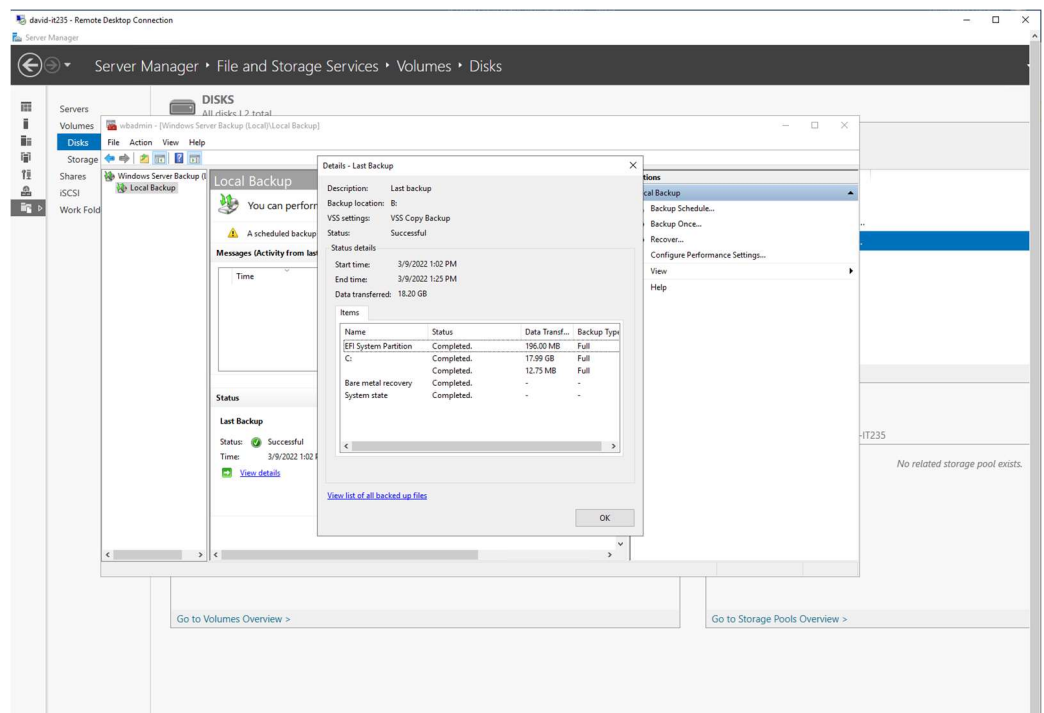
- Using my VMware, I added another 30 GB virtual hard disk to my virtual machine running Server and store the file as a single file.
- Using Windows Server, I created a simple volume (Backup) using NTFS.
- All other dialog box prompts I used their default setting in each of their section.
- I install Windows Server Backup using Server Manager.
 - By using the Backup Once Wizard I was able to perform a one-time full server backup to the Backup volume I created.



In addition to the above I need to address the following question;

- What is backed up as a result of using a Full Server Backup?

As the name implies, this type of backup makes a copy of all data to a storage device, such as Bare metal recovery, System state, C:, EFI etc. The primary advantage to performing a full backup during every operation is that a complete copy of all data is available with a single set of media.



➤ What is recoverable as a result of using the Full Server Backup?

The entire data are recoverable using full backups as they are more reliable in case of data corruption or breakage. A full backup is creating one or more copies of all organizational data files in a single backup operation to protect them. Before the entire backup process, a data protection specialist such as a backup administrator designates the files to be duplicated — or all files are copied

Users and Groups for Active Directory

Active Directory stores users and groups in a folder called Users within Active Directory Users and Computers. Each of the items in the left pane is a container. Active Directory is logically set out so that thousands of objects can be organized and found. Each object must be in a container. Active Directory is logically set out so that thousands of objects can be organized and found. Each object must be in a container. Containers may themselves contain containers! Users and groups can be created in any container.

1. I will be using Active Directory Users and Computers to creating the following new Organizational Units (OUs):
 - Finance Team
 - HR Team
 - Technical Team
 - Administration Team
2. I will be using Active Directory Users and Computers to creating the following Groups:
 - Finance
 - HR
 - Technical
 - Administrative
3. I will be using Active Directory Users and Computers to create the following new users:
 - Michelle P. Lucifer
 - Timothy A. Merrow
 - Jason C. Jankowski
 - Germaine S. Smith
 - Marilyn B. Brown
 - Joseph B. Steinhoff
 - Micheal C. Roop
 - James M. Rodrigues
 - John P. Ridgway
 - Branda J. Soto

- Judith J. Keller
 - Shirley W. Henderson
 - David P. Perez
 - Jimmie V. Robertson
 - Anna J. Kelley
 - Barbara S. Overby
4. Using Active Directory Users and Computers to create the following users Groups
- Finance Group in Finance Team OUs
 - Technical Group in Technical Team OUs
 - HR Group in HR Team OUs
 - Administrative Group in Administrative Team OUs
 - Backup Groups in PL.com AD
 - Disaster Recovery Group in PL.com AD
5. Using Active Directory Users and Computers to assign the following users to the following Organization Unit
- Michelle P. Lucifer, Timothy A. Merrow, Jason C. Jankowski, and David P. Perez to Finance Team Organization Unit
 - Germaine S. Smith, Marilyn B. Brown, Joseph B. Steinhoff, and Jimmie V. Robertson to Technical Team Organization Unit
 - Michael C. Roop, James M. Rodrigues, John P. Ridgway, and Anna J. Kelley to HR Team Organization Unit
 - Branda J. Soto, Judith J. Keller, Shirley W. Henderson, and Barbara S. Overby to Administrative Team Organization Unit
6. Using Active Directory Users and Computers to assign the following users to the following Groups which is first created based on the role of users
- Michelle P. Lucifer, Timothy A. Merrow, Jason C. Jankowski, and David P. Perez to Finance Group
 - Germaine S. Smith, Marilyn B. Brown, Joseph B. Steinhoff, and Jimmie V. Robertson to Technical Group
 - Michael C. Roop, James M. Rodrigues, John P. Ridgway, and Anna J. Kelley to HR Group

- Branda J. Soto, Judith J. Keller, Shirley W. Henderson, and Barbara S. Overby to Administrative Group
- Michelle P. Lucifer, Germaine S. Smith, Marilyn B. Brown, Joseph B. Steinhoff, and Jimmie V. Robertson, Michael C. Roop, and Branda J. Soto to Backup Group
- Michelle P. Lucifer, Germaine S. Smith, Jimmie V. Robertson, Michael C. Roop, and Branda J. Soto to Disaster Recovery Group

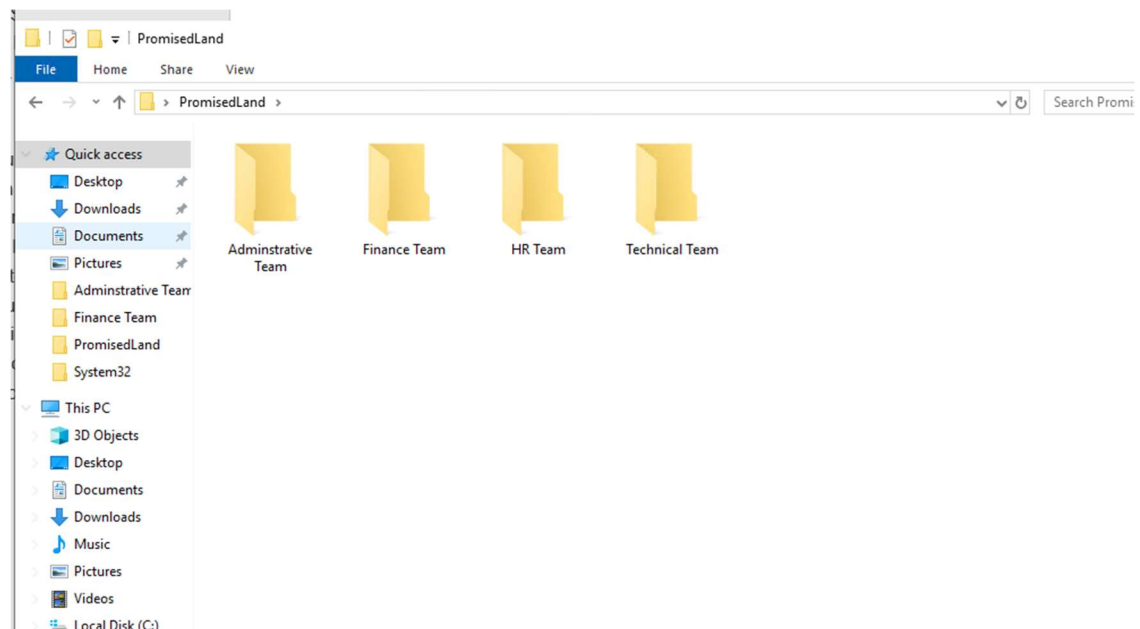
In summary, users and groups in the active directory are responsible for allocating each organization member to their respective department.

Organizational units (OUs) in an Active Directory Domain Services (AD DS) managed domain to let you logically group objects such as user accounts, service accounts, or computer accounts. You can then assign administrators to specific OUs and apply group policy to enforce targeted configuration settings. OUs are unique from Containers, another type of organizational object contained within Active Directory. OUs differ from Containers primarily because an OU can have a Group Policy Object (GPO) linked to it, whereas a Container cannot.

Principle of Least Privilege (POLP)

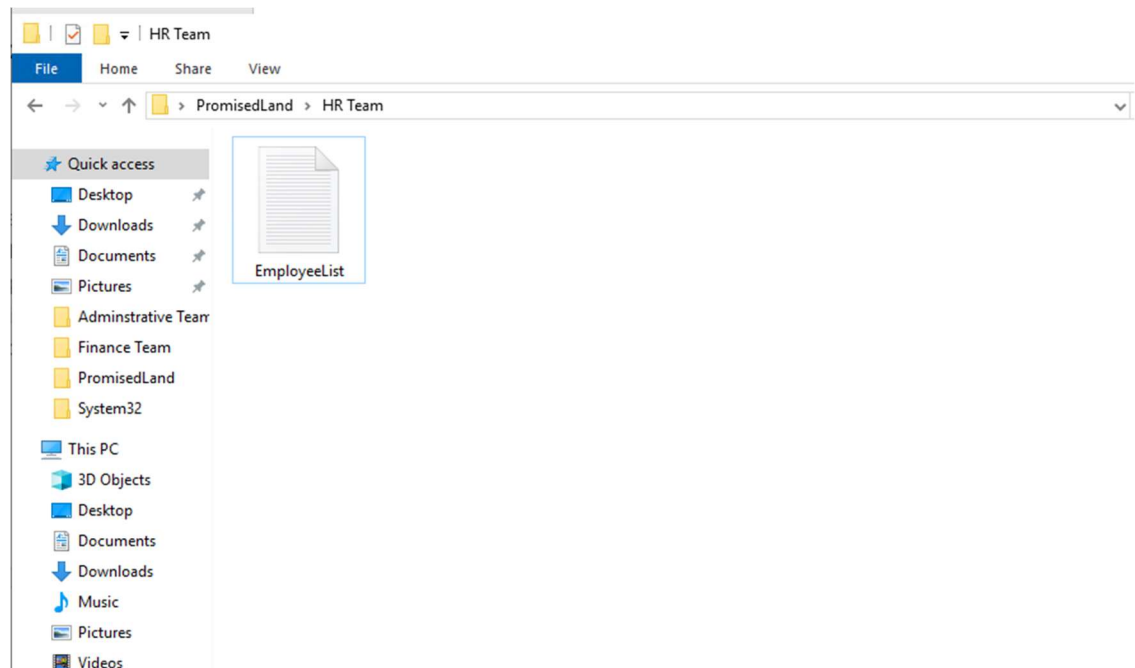
As a server (systems) administrator, you will need to be able to protect data by limiting access to that data. The principle of least privilege (POLP), an important concept in security, is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under POLP, users are granted permission to read, write, or execute only the files and resources they need to do their jobs—or, the least amount of privilege necessary. In this aspect of the project, I will be using the following steps to implement the principle of least privilege (POLP) using the information available on the organization chart.

1. Using File Explorer to create the PromisedLand folder:
2. Create the following subfolders within the PromisedLand folder:
 - Finance
 - HR
 - Technical
 - Administrative

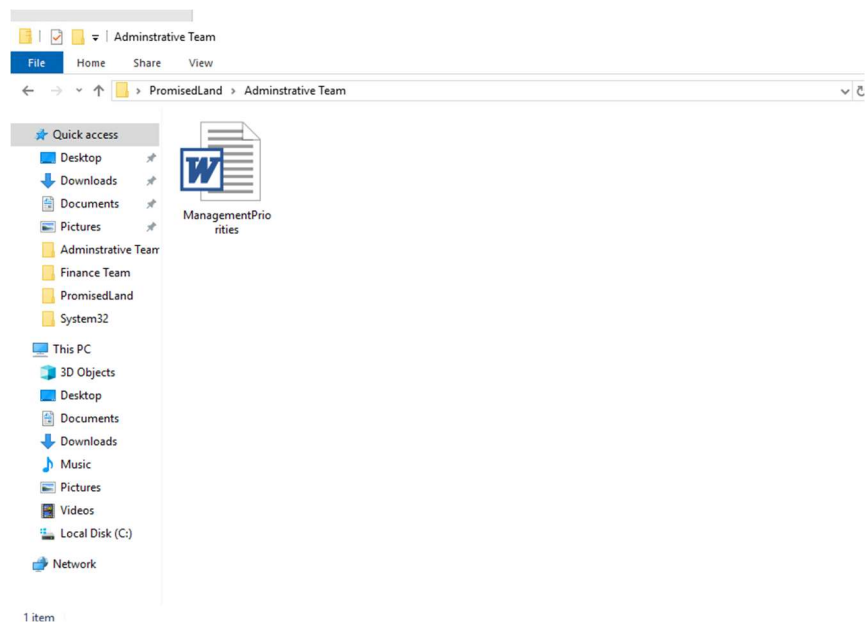


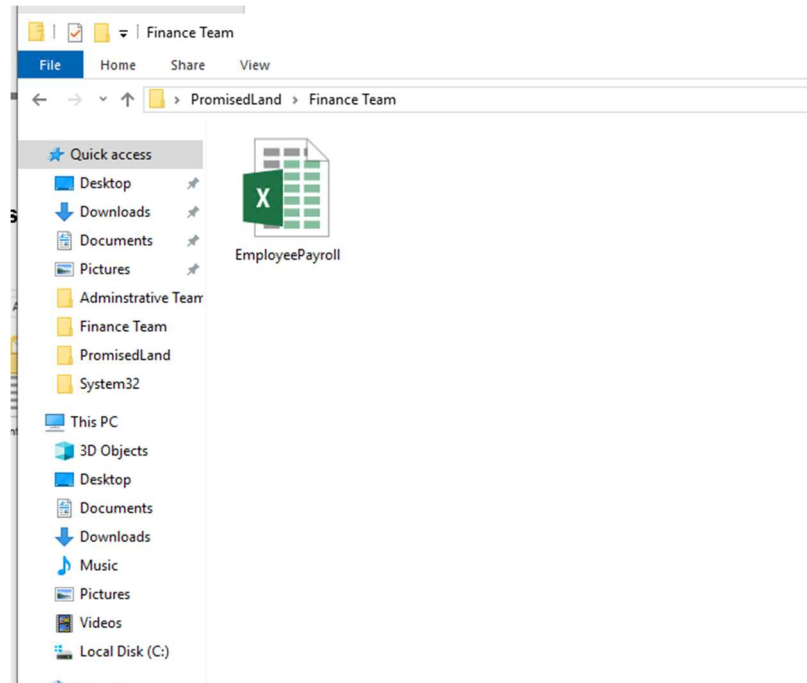
3. Create the following file within the subfolders

“EmployeeList.txt” in the HR folder



“ManagementPriorities.docx” in the administrative folder



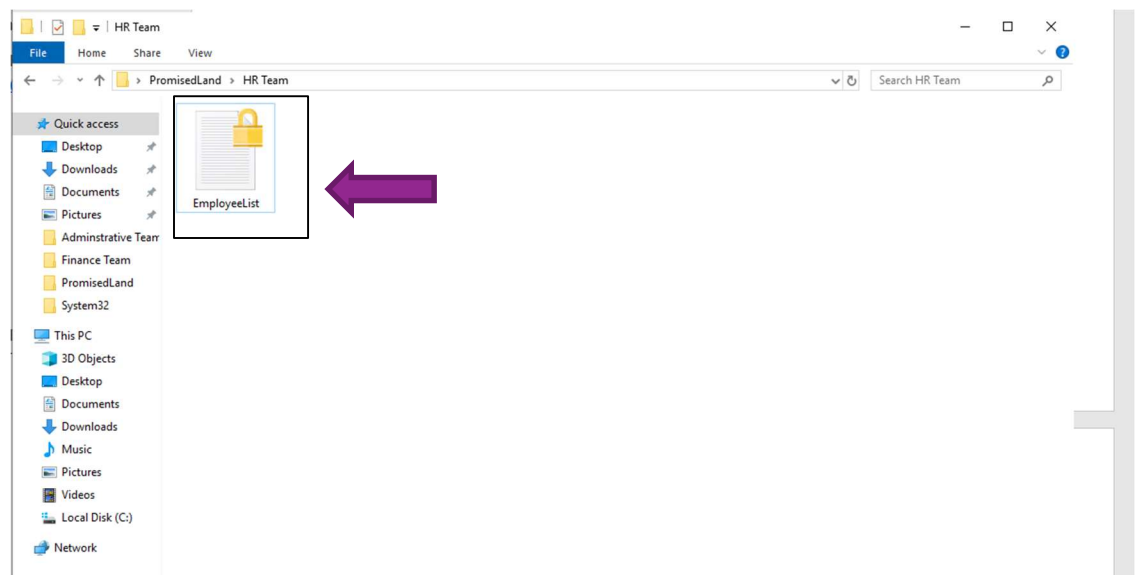
“EmployeePayroll.xlsx” in the Finance folder

In summary, assigning users to its respective department ensures the effectiveness and delivery of its user's initial engagement, which is their primary assignment and responsibility to the organization. Furthermore, each user is assigned responsibility based on their group, which minimizes the workload and produces effective service delivery by members.

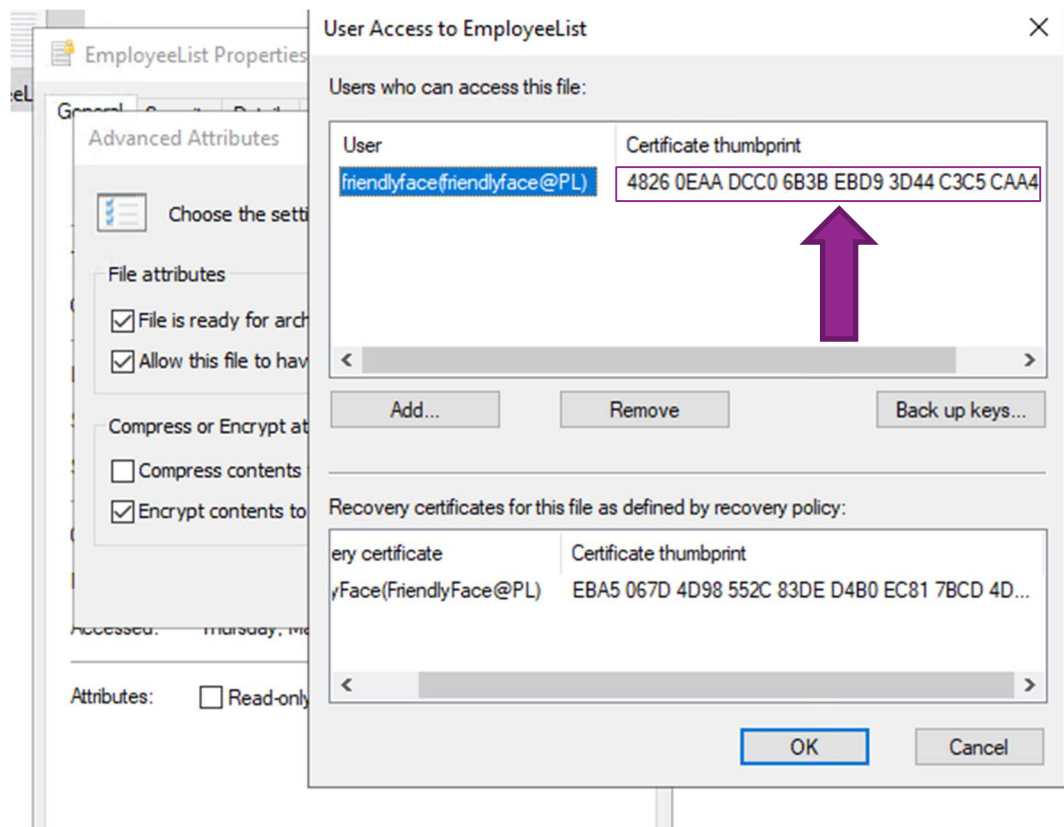
Encrypted File System

An encryption system in the Windows NTFS file system, starting with Windows XP Pro. EFS enables users to encrypt their data in storage using a password. EFS is a user-based encryption control technique that enables users to control who can read the files on their system. The typical method of using EFS is to perform encryption at the folder level. EFS ensures that all files added to the encrypted folder are automatically encrypted. I will be using the following steps to implement the Encrypted File System (EFS) using the information available on the principle of least privilege (POLP) with the steps below;

1. Encrypt each file created using EFS in [Principle of least privilege \(POLP\)](#) Evidence of encrypted file below



2. Below is a display of EmployeeList.txt showing the Certificate Thumbprint



Users who can access the encrypted file

EFS provides users with access privileges to those who have the right or give them access to the specific file and folder. EFS ensures secured files and limits the access or blocks unauthorized users' access to files that EFS encrypts. EFS generates certificates that allow only users with the private key to access the file. Using an Encrypted file system further adds a layer of security to the file and thus further ensures that users with the proper privileges are given access to the file. EFS protects the file integrity and ensures the delivery of shared files is visible to those who have the access right to such files.

Security Protection

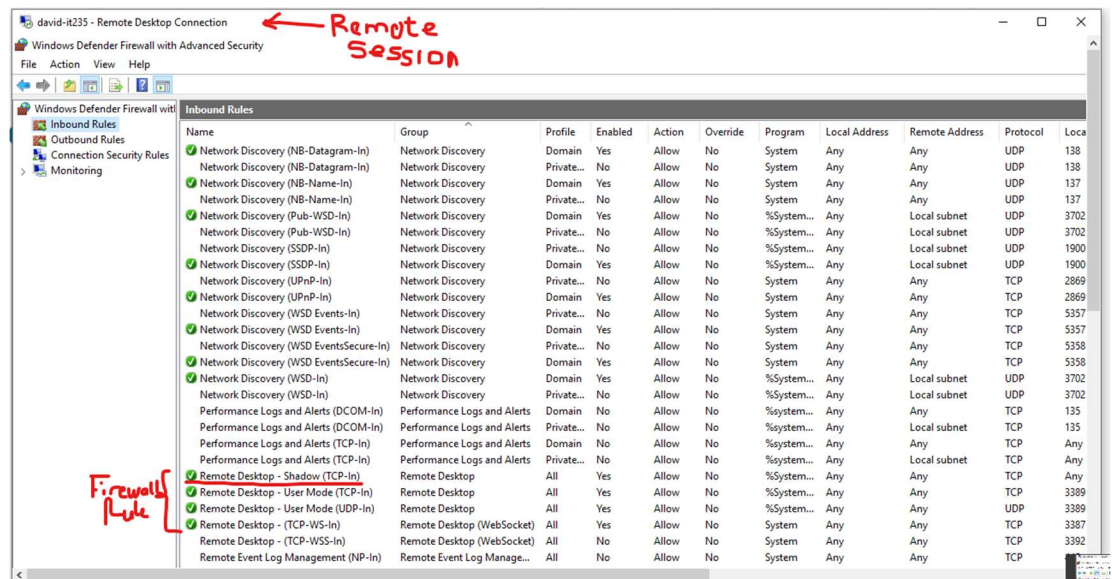
In this aspect of the project, I have classified the security apparatus into the following;

Network Security

This aspect of the security protection ensures system security alongside users authentication, access control list (ACL), Network Intrusion Detection System, Lightweight Directory Access Protocol (LDAP), VPN, encryption, and alike. For this exercise am expected to do some configurations to meet the requirement for this assignment which are;

Firewall rule and allow Remote Desktop Protocol User Mode

I will be configuring a host-based firewall rule to allow Remote Desktop Protocol User Mode for the PL.com domain. Remote Desktop is a client application that allows a “client” computer to connect to a “host” computer from a remote location. Users can then control and use the applications and files on the host device anywhere. To achieve this, I created the firewall rule that allows the remote connection through the inbound rule that enables the Remote Desktop (TCP), which enables me to connect with the PromisedLand server in the VMware. Below is an illustration of the connection and remote session to PromisedLand Server.



Access Control List and Why PromisedLand Should use it

I will be explaining what an access control list is used for and why PL.com should use it. An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular system resource. They are also installed in routers or switches, where they act as filters, managing which traffic can access the network. By controlling how many users can access specific files or systems, access control lists limit network traffic and increase network performance. ACL saves companies money because they can get the most out of their current network instead of regularly upgrading and increasing their network. Cost is an essential factor when it comes to most companies and industries. Every good manager would want to spend less and gain more from their investment. It is a nature of business, and PromisedLand is not an exception.

Network Intrusion Detection System

I will be explaining Network Intrusion Detection System and Why I would recommend placing it in PL.com's network. A network intrusion detection system is a device or software used to monitor the network for malicious activity or policy violations. Any malicious activities are quickly flagged and recorded for the network administrator to take appropriate steps to eliminate the threats. The best place to put an intrusion detection system IDS would be

behind the firewall. This is because IDS is an extra layer of security to ensure the integrity of system transactions and communication.

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is used to access a network directory and the port used by LDAP. The Lightweight Directory Access Protocol (LDAP) is a vendor-neutral application protocol used to maintain distributed directory information in an organized, easy-to-query manner. LDAP uses a relatively simple, string-based query to extract information from Active Directory. It can also store and extract usernames and passwords in Active Directory and share with connected devices or applications. The default port for LDAP is port 389.

Encrypting the Communications in PL.com

I will encrypt the communications in PL.com, the difference between public and private keys, and provide one example where PL.com could use digital certificates and describe why they would want to use the example. Encryption is data conversion from a readable format into an encoded format. Encrypted data can only be read or processed after it's been decrypted. Encryption is the basic building block of data security and ensures the originality of the content shared on the network. PromisedLand information shared is decrypted by the other device with the decrypting key. The private key is used to encrypt and decrypt the data and is shared between the sender and receiver of encrypted data. The public key is only used to encrypt data and is free to use, and the private key is kept secret only. The PromisedLand Domain would use Encrypting File System (EFS) to share information on the network. EFS generates certificates that the intended user can only decrypt on the network. Its further used to ensure an extra layer of security with information sharing on the network. For example, when a file is shared for a group with limited access, the ES provides this security by ensuring that the intended users have access to the security file. If anyone other than the intended user tries to access such a file, it will be denied access to the file.

Two Reasons why VPN are useful to PL.com

I will Identify two reasons why VPNs are useful to PL.com. VPN is a virtual private network that extends a private network across a public network. It enables users to send and receive data across shared or public networks is directly connected to the private network. the two main reason why VPN would be beneficial to PromisedLand are;

1. VPN disguises user data traffic online and protects it from external access
2. VPN is a secure and private network connection through the public internet

How VLAN secure data on a network

I will be explaining how VLAN help to secure data on a network. VLANs limit the ability of any device to hear anything on other Virtual Local Area Networks. For example, VLANs are often used for virtual workgroups on a corporate network because they make it easier to place geographically-dispersed members together. VLAN creates the avenue for an administrator to assign each department VLANs, allowing only those within the VLAN to communicate with each other and does not allow an external machine on another network to hear the communication within the VLAN. VLAN helps limit the broadcast of messages within the same VLAN.

Physical Security Methods and Concepts

The second aspect of the security protection it deals with is how to deal with the physical security features needed to ensure the safety of PromisedLand data centers. The security features needed to be addressed in this exercise include:

- Mantrap.
- Environmental assessment with security.
- Multi-factor authentication on one of my accounts.

I have decided in addressing exercise in the following pattern which are;

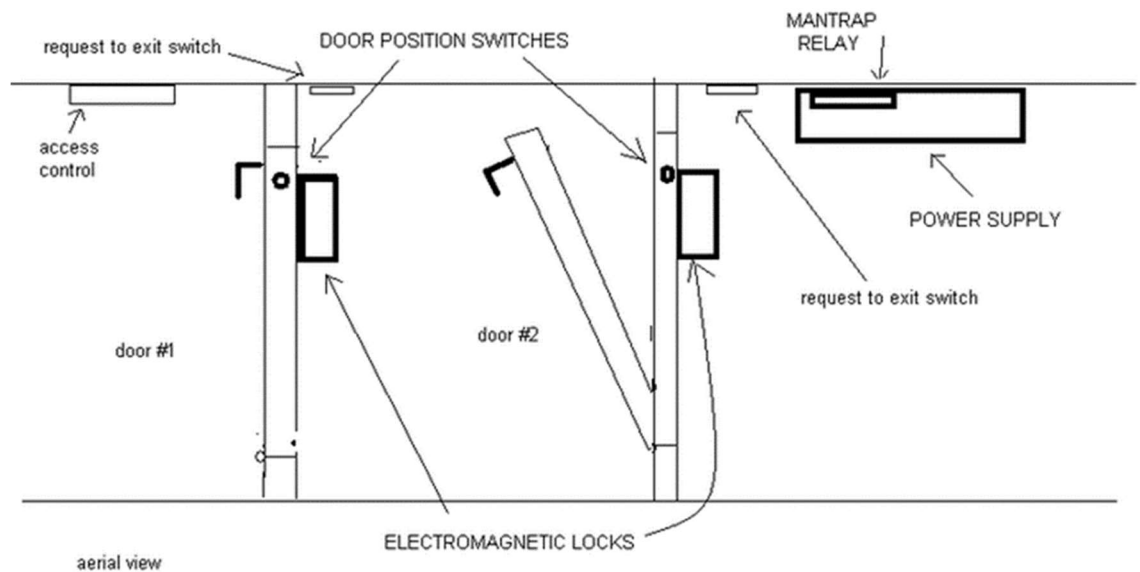
PromisedLand implementing the use of a mantrap in their data centers

I envision PromisedLand implementing a mantrap in their data centers, and I will show images of a mantrap that clearly explains how mantrap works.

Mantrap is a locking system that prevents one door from opening before another is closed. One top-rated application for a mantrap is in a clean room, where it is vital to control the flow of air in and out of the secured space.

Mantrap works in the following manner; a person activates the access control (keypad, pushbutton switch, key switch, prox reader, etc.). The access control closes a contact on the mantrap relay for about 10 seconds depending on the configuration, telling it to unlock the first door for that amount of time. The person opens the door, changing the state of the door position switch, which tells the mantrap relay to keep the second door locked. When the first door closes, the door position switch on the first door returns to its original state, signaling the mantrap relay to release the second door. When the person opens the second door, it changes the state of the door position switch on the second door, which tells the mantrap relay to keep the first door locked. When the second door closes, and the door position switch on it returns to its original state, the mantrap relay relocks both doors. The data center is the powerhouse of information about any organization. Keeping the environment extremely secure would be an essential aspect of any organization. If PromisedLand

makes use of a mantrap helps to add additional physical security to limit access to its data center



I could use three physical security controls to protect PromisedLand Server from outside threats. I will be using industrial recognized physical security measures and the environment where my computer resides and identify three security controls that protect the PromisedLand server from outside threats. The three security controls I identified are as follows;

1. Closed-circuit television (CCTV) camera surveillance

These days, most organizations and businesses use additional means of surveillance apart from human security. The CCTV cameras help to enhance the security apparatus established in an organization. The CCTV camera help to ensure physical security measures. They provide instant or periodic records of every activity in a secure location, and these records are used as evidence in law courts. They say pictures worth a thousand words, it is confirmed as the CCTV provide proof of actions or activity carried out. Its why it is one of the security measures I found effective in my current location.

2. Uninterruptible power supply (UPS)

The other physical security measure I can identify within my environment is an uninterruptible power supply. Electricity is an essential component that makes most businesses operate, for example. Most apparatus depends on this essential factor to operate; failure in light would lead to the collapse of the entire operation of the business. With this in mind, most businesses put in structures that guarantee fail-proof to ensure safety and prevent data loss. The server provides services for other computers either remotely or locally, so the server is going off means that such services would not be available when the server goes off due to a power outage. With this in mind, this is a significant reason why UPS provides an alternative means to sustain the system until the power outage is fixed. Based on these facts, It's the second essential security measure I found effective in my current location.

3. Cooling System

The cooling system is essential for system security, which often leads to system failure and data loss as most businesses and organizations find this effective in their data center. The server provides services in a resource center for another computer that uses its vast resources. Using these resources on the server, the server load increases, and the processor is used up. Thus, the heat that emanates from the server continues to grow. If this heat is not adequately managed, they pose a security issue to other users on the server due to system failure. Heat is a significant factor in any computer setup center as the proper cooling system provides smooth services and prevents data loss and system crashing.

Implementing an additional multi-factor authentication on my personal accounts

I will be implementing one additional multi-factor authentication on one of my accounts. To show how two-factor authentication can secure more of its staff activity through this authentication. (For example, the churchofjesuschrist.org, Gmail, or Apple account.) Two-factor authentication is an authentication mechanism to double-check account user identity is legitimate. Two-factor

authentication works are as follows; When a user wants to sign in to their account, the user is prompted to authenticate with a username and a password - the first verification layer. Two-factor authentication works as an extra step in the process, a second security layer that will re-confirm the user's identity is legitimate. Its purpose is to make attackers' life harder and reduce fraud risks.

Server Hardening

As a server (system) administrator, there would be a time to implement server hardening techniques. System hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. System hardening aims to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. In this aspect of the project, I will identify four server hardening techniques that PromisedLand can use on their physical and virtual servers to reduce potential risk or lead that makes the system vulnerable.

Computer security is a situation of preventing and detecting unauthorized users of an organization's computer. We do this to prevent unauthorized access to the company's computer. Once a computer is infiltrated or accessed by unauthorized users, abuse is inevitable. Once they gain access to a computer, Malicious users exploit the machine until discovered.

Disadvantages of computer security configuration

1. Firewalls can be difficult to configure correctly.

One of the significant challenges in the security system is its configuration, as it defines the strength and vulnerability. Therefore, proper configuration must be ensured to achieve maximum security at the firewall level.

2. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.

When there is a loophole in the firewall configuration, the whole system setup is vulnerable. A malicious hacker is looking for a system to gain access to the machine and compromise the security system.

3. Makes the system slower than before.

The security system requires verification before they give access to users. So system delivering speed concerning the security level set for the whole machine. It's unfortunate that users hardly notice because computer systems

do this at a relatively high speed that is hardly noticed unless it's being viewed through a network packet tracer.

4. Need to keep updating the new software in order to keep security up to date.

Hackers are developing new means of gaining access to an already existing system. Therefore, software developers are constantly building up their software security to meet the threats to their systems.

5. Could be costly for average user.

System security requires expertise to implement. Thus, there is a need to hire a professional, which is quite expensive for average business owners.

Implication of Services on computer security

Services run in the background without a user interface and enable system features (such as printing, networking, remote access, File Explorer, Windows Search, updates, etc.) and apps to operate as intended. These running programs if they are not monitored or in used, some may even open ports which could lead system vulnerability. I will be using the Disabling System Services on Windows Servers and disable the following services on the Windows virtual server:

1. **Bluetooth Support Service:** The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated.
2. **CDPUserSvc:** It's used to make a connection with Bluetooth devices easier. It is a new service that has only been found in Windows 10, it's advised to disable the process by modifying users registry.
3. **DmwAppUshSvc:** Its display name is "Device Management Application Protocol (WAP) Push message Routing Service." Its Description is:

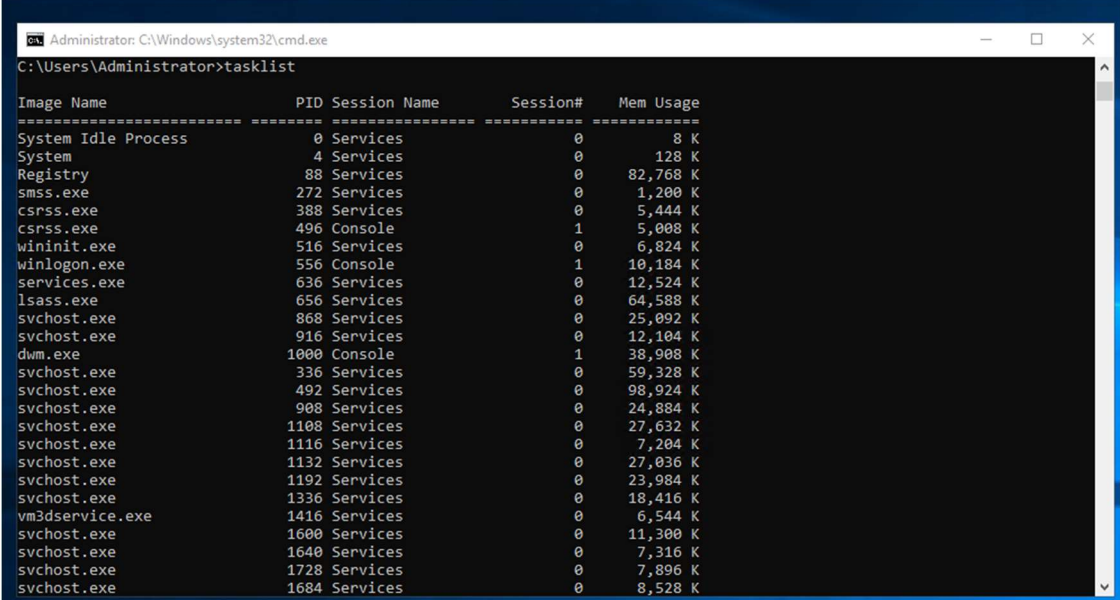
Routes Wireless Application Protocol (WAP) Push messages received by the device and synchronizes Device Management sessions.

4. **Download Maps Manager:** Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps.
5. **Geolocation Service:** Geolocation marketing determines the location of a computer, phone, or other network-based devices. This inferred location is based on geographical measurements of latitude and longitude to narrow down the location to city, zip code, street, and even address.
6. **Internet Connection Sharing (ICS):** Internet Connection Sharing (ICS) is a feature that allows a device with internet access to act as a host or access point for other devices to connect to the web.
7. **Link-Layer Topology Discovery Mapper:** Link-Layer Topology Discovery Mapper I/O Driver. Used to discover other computers connected to your local network. Link Layer Topology Responder. Used to identify your computer to other computers connected to your local network.

Ports in use by programs on the Windows Server

The following ports are used by the server and the application by default since non-Microsoft application applications are yet to be installed on the server.

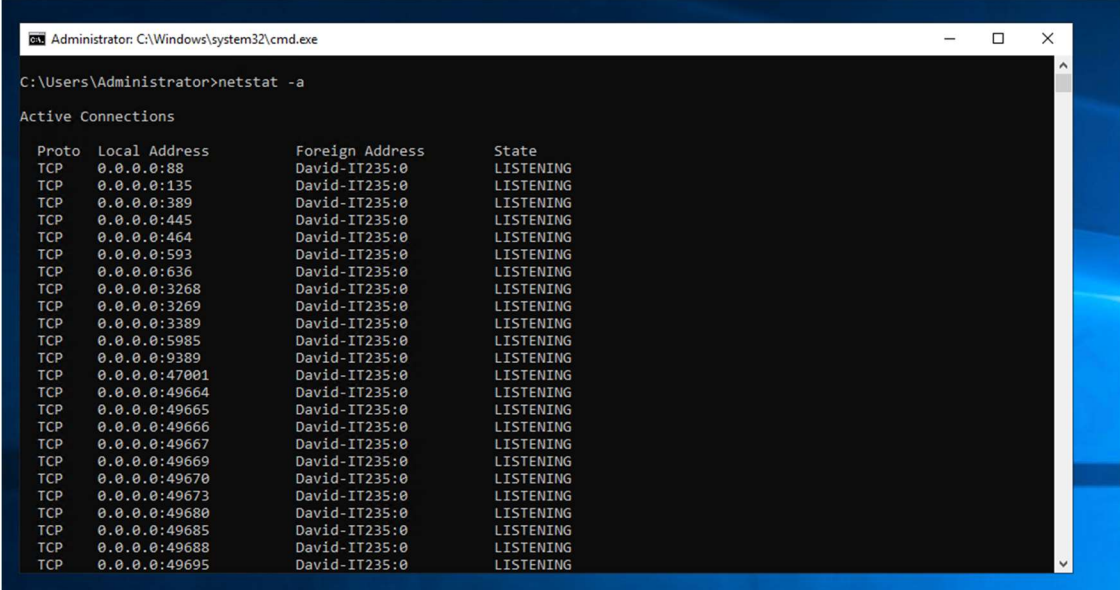
Using Tasklist command



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>tasklist

Image Name                    PID Session Name        Session#    Mem Usage
=====
System Idle Process           0 Services             0             8 K
System                        4 Services             0            128 K
Registry                      88 Services            0          82,768 K
smss.exe                     272 Services            0           1,200 K
csrss.exe                    388 Services            0           5,444 K
csrss.exe                    496 Console             1           5,008 K
wininit.exe                  516 Services            0           6,824 K
winlogon.exe                 556 Console             1          10,184 K
services.exe                 636 Services            0          12,524 K
lsass.exe                    656 Services            0          64,588 K
svchost.exe                  868 Services            0          25,092 K
svchost.exe                  916 Services            0          12,104 K
dwm.exe                     1000 Console             1          38,908 K
svchost.exe                  336 Services            0          59,328 K
svchost.exe                  492 Services            0          98,924 K
svchost.exe                  908 Services            0          24,884 K
svchost.exe                 1108 Services            0          27,632 K
svchost.exe                 1116 Services            0           7,204 K
svchost.exe                 1132 Services            0          27,036 K
svchost.exe                 1192 Services            0          23,984 K
svchost.exe                 1336 Services            0          18,416 K
vm3dservice.exe             1416 Services            0           6,544 K
svchost.exe                 1600 Services            0          11,300 K
svchost.exe                 1640 Services            0           7,316 K
svchost.exe                 1728 Services            0           7,896 K
svchost.exe                 1684 Services            0          8,528 K
```

Using Netstat command



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP 0.0.0.0:88              David-IT235:0          LISTENING
TCP 0.0.0.0:135             David-IT235:0          LISTENING
TCP 0.0.0.0:389             David-IT235:0          LISTENING
TCP 0.0.0.0:445             David-IT235:0          LISTENING
TCP 0.0.0.0:464             David-IT235:0          LISTENING
TCP 0.0.0.0:593             David-IT235:0          LISTENING
TCP 0.0.0.0:636             David-IT235:0          LISTENING
TCP 0.0.0.0:3268            David-IT235:0          LISTENING
TCP 0.0.0.0:3269            David-IT235:0          LISTENING
TCP 0.0.0.0:3389            David-IT235:0          LISTENING
TCP 0.0.0.0:5985            David-IT235:0          LISTENING
TCP 0.0.0.0:9389            David-IT235:0          LISTENING
TCP 0.0.0.0:47001           David-IT235:0          LISTENING
TCP 0.0.0.0:49664           David-IT235:0          LISTENING
TCP 0.0.0.0:49665           David-IT235:0          LISTENING
TCP 0.0.0.0:49666           David-IT235:0          LISTENING
TCP 0.0.0.0:49667           David-IT235:0          LISTENING
TCP 0.0.0.0:49669           David-IT235:0          LISTENING
TCP 0.0.0.0:49670           David-IT235:0          LISTENING
TCP 0.0.0.0:49673           David-IT235:0          LISTENING
TCP 0.0.0.0:49680           David-IT235:0          LISTENING
TCP 0.0.0.0:49685           David-IT235:0          LISTENING
TCP 0.0.0.0:49688           David-IT235:0          LISTENING
TCP 0.0.0.0:49695           David-IT235:0          LISTENING
```

Anti-malware software is installed by default on a Windows Server?

Microsoft Defender Antivirus is free and included in Windows, always on and working to protect PC against malware. Hackers and scammers sometimes

use fake antimalware software to trick you into installing viruses or malware on your computer. Microsoft Defender Antivirus is free and included in Windows, always on and working to protect your PC against malware. Hackers and scammers sometimes use fake antimalware software to trick you into installing viruses or malware on your computer.

Nobody will like to use a vulnerable system as it breaks its integrity for further use unless the security issues are addressed first. It is one of the reasons why security is an essential aspect of every organization, as it is responsible for business integrity and checks. There is a need for maximum security measures to reduce the risk of security floors. Security hardening does not ensure total security but reduces the risk of making the system vulnerable.

Disaster Recovery

A disaster recovery plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies the procedures an organization is to follow in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during, and after a disaster. Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan (sometimes erroneously called a continuity of operations plan) is increasingly associated with the recovery of information technology data, assets, and facilities. The DRP I will be discussing at this aspects include the following;

- HIGH-LEVEL OUTLINE OF DISASTER RECOVERY PLAN
- KEY PERSONNEL AND CONTACT INFORMATION
- INFORMATION SERVICES BACKUP PROCEDURES
- DISASTER RECOVERY PROCEDURES
- RECOVERY PLAN FOR COLD SITE
- RECOVERY PLAN FOR HOT SITE
- RESTORATION PROCESS
- RECOVERY PLAN PRACTICE AND EXERCISING
- DISASTER SITE REBUILDING
- PLAN CHANGES OR UPDATES

HIGH-LEVEL OUTLINE OF DISASTER RECOVERY PLAN

The principal aim of this disaster recovery plan (DRP) is to provide a detailed plan to reduce loss to PromisedLand. This plan will minimize interruptions to normal operations. It will also allow us to limit the impact of the disaster and minimize the finance loss of PromisedLand. The DRP will help personnel in the emergency procedures smoothly move from the disaster to business continuity as the system downtime always results in financial loss.

KEY PERSONNEL AND CONTACT INFORMATION

NAME & TITLE	ROLE	PHONE	EMAIL
Mikey Davis	CEO	0245685901	mdavis@PL.com
Michelle P. Lucifer	Financial Manager	0245654520	mlucifer@PL.com
Timothy A. Merrow	Financial Senior Manager	0254878985	tmerrow@PL.com
Jason C. Jankowski	Financial Assistant Manager	0564569865	jjankowski@PL.com
Germaine S. Smith	Information System Technical Manager	0265987895	gsmith@PL.com
Marilyn B. Brown	Information System Senior Manager	0265897852	mbrown@PL.com
Joseph B. Steinhoff	Information System Assistant Manager	0254698756	jsteinhoff@PL.com
Micheal C. Roop	Human Resources Manager	0545698756	mroop@PL.com
James M. Rodrigues	Human Resources Senior Manager	0254568545	jrodrigues@PL.com
John P. Ridgway	Human Resources Assistant Manager	0569875654	jridgway@PL.com
Branda J. Soto	Administrative Manager	0254789856	bsolo@PL.com
Judith J. Keller	Administrative Senior Manager	0545654123	jkeller@PL.com
Shirley W. Henderson	Administrative Assistant Manager	0545212325	shenderson@PL.com
David P. Perez	Financial Staff	0546523252	dperez@PL.com
Jimmie V. Robertson	Information System Staff	0524565232	<u>jrobertson@PL.com</u>

Anna J. Kelley	Human Resources Staff	0254565478	akelley@PL.com
Barbara S. Overby	Administrative Staf	0254565450	boverby@PL.com

INFORMATION SERVICES BACKUP PROCEDURES

PromisedLand data will be on a secure backup plan carried out automatically. This backups system ensures the series of system backups every 2 hours interval, which means 12 times in 24 hours. The backup is saved in a remote site located in Missouri, USA, using a cloud backup, limiting the essence of data loss. The cloud backup protects the company's data loss from natural disasters or cyberattacks that may affect PromisedLand's data center. The backup is maintained by an Information System Staff, which validates and tests before implementing the backups.

DISASTER RECOVERY PROCEDURES

In case of emergency Germaine S. Smith (Information System Technical Manager) coordinates alongside the team in his department to ensure that the entire disaster recovery plan return of business continuity depending on the incidence level of priority which are;

- **Low-Level Priority:** The low-level priority deals with the disruption of services due to power outages or other minus issues that do not exceed 2 hours or more but less than 24-hour disruption.
- **High-Level Priority:** When the disruption of services exceeds 24 hours or more than a day but less than a week. This disruption may be a result of cyber attacks or other measures.
- **Critical Level Priority:** This is when the disruption of services exceeds more than a week. This disruption may be due to natural disasters and other physical incidents that humans cannot control.

RECOVERY PLAN FOR COLD SITE

The Low and High-Level incident priority will use the mobile site due to its ability to provide immediate solutions in case of disaster. They do this because they save data in tapes and readily available storage, which means it is readily available to remediate the situation at hand. For this reason, it seems to be the first approach in providing solutions when disaster strikes. They are managed by Information System Staff, which validates and tests before implementing the backups.

RECOVERY PLAN FOR HOT SITE

The High and Critical Level incident priority will use the Hot site due to its significant influence. They do this because cloud storage provides an effective and reliable backup means. After all, they are not influenced by natural disasters or any disasters. They are managed by Information System Senior Manager, which validates and tests before implementing the backups. The Information System Manager, who is the departmental head in Information System Units, approves the implementation of backups of the IT departments.

RESTORATION PROCESS

The IT departments managed all backups and system restoration. All the restoration processes will be managed by the Information System Manager, the departmental head in IT departments, and approves the restoration from the backups of in it departments. Before implementing the restoration from the backups, information accessibility will be available to a department member to update staff and members of the PromisedLand on the current status of the organization's restoration process.

RECOVERY PLAN PRACTICE AND EXERCISING

These activities will be conducted weekly to see how the system would perform if faced with an absolute disaster that threatens the disruption of services and operations. There will be a routine check on the activities on the backup side and continuous testing of the system security integrity, which the IT departments manage. It will give room for proper management of the overall

activities of the system, which in turn affects the checks on system performance and integrity.

DISASTER SITE REBUILDING

The IT department works with another department within the PromisedLand to achieve proper site rebuilding. The essence of this is to ensure services restored are fully functioning to expectation. The IT department head would spearhead the management of this function by allocating members within his team to collaborate with other departmental heads to contribute to rebuilding and maintaining stability.

PLAN CHANGES OR UPDATES

Like any other organization, staff may be moved from one location to another. In that vein, the department managing the disaster recovery needs to put subsequent staff who will foster the change in the system. There is a need for this action because it ensures that systems are maintained and sustained. The IT departmental head makes sure his team members are involved in all the activities to ensure things are carried out as expected.

In summary, a disaster recovery plan is crucial for the server administrator to ensure these prerequisites are adequately documented and in place if disaster strikes. There is no such thing as perfection, so there would be a need for constant review of the DRP as it will help to be updated to dates and keep the information fresh as soon as possible to make it available to team members when needed. The DRP should contain crucial aspects of the DRP, such as the backup procedures and plans for recovery, including the onsite and offsite storage to keep the company's data safe in case of natural disaster or another form of disaster.

Cost of Recommended Servers for small businesses

The prices I will share are servers recommended to small businesses or a start-up size since the number of employees is 45. Each of the servers can offer a significant amount of support to the PromisedLand. The server is;

1. [Dell. PowerEdge T30.](#)
2. [Dell. PowerEdge T20 \[barebones\]](#)
3. [Lenovo. ThinkServer TS150.](#)
4. [HPE. ProLiant ML350 Gen 10.](#)
5. [Fujitsu. Primergy TX1310 M1.](#)
6. [HP. ProLiant Microserver Gen8.](#)
7. [Lenovo. ThinkServer TS460.](#)
8. [HP. ProLiant ML350 G9 5U.](#)

Dell. PowerEdge T30

The ideal first server for small offices and home offices (SOHO), the PowerEdge T30 packs sizable internal storage. capacity and capable performance into a compact, quiet, mini-tower chassis that delivers efficient, worry-free operation.

How much is Dell PowerEdge T30?
Compare with similar items

This item 2017 Newest Dell PowerEdge T30 Tower Server System| Intel Xeon E3-1225 v5 3.3GHz Quad Core| 8GB RAM | 1TB HDD| DVD RW | No Operating System | Black

Price	From \$848.98
Sold By	Available from these sellers
Computer Memory Size	8 GB
CPU Model	Xeon E3 1225

Dell. PowerEdge T20 [barebones]

The Dell PowerEdge T20 tower server is designed for a small business office environment or the home. For an entry-level server, it offers a surprisingly large storage capacity plus enterprise-class features, including Intel Xeon processors and ECC memory for resiliency



Dell PowerEdge T20 Tower Server, Intel Xeon Quad Core 3.2GHz, 16GB, 4TB SATA (Renewed)

[Visit the Amazon Renewed Store](#)

Price: \$1,199.00

Product works and looks like new. Backed by the 90-day Amazon Renewed Guarantee.

- This pre-owned product has been professionally inspected, tested and cleaned by Amazon-qualified suppliers.
- There will be no visible cosmetic imperfections when held at an arm's length.
- Products with batteries will exceed 80% capacity relative to new.
- Accessories may not be original, but will be compatible and fully functional. Product may come in generic box.
- This product is eligible for a replacement or refund within 90 days of receipt if you are not satisfied under the Amazon Renewed Guarantee. [See terms here.](#)

Personal computer design type Computer Tower
Series ASISVR66
Ram Memory Installed Size 16 GB
Operating System None
[See more](#)

\$1,199.00

Your selected delivery location is beyond seller's shipping coverage for this item. Please choose a different delivery location or purchase from another seller.

[Deliver to Ghana](#)

See similar items shipping to Ghana.

[See Similar Items](#)

Share [Facebook](#) [Twitter](#) [Pinterest](#)



Dell PowerEdge R720xd Server 2...
\$1,341.20 [prime](#)

Sponsored

And the mini-tower below

Dell PowerEdge T20 Mini-Tower Server Specifications & Pricing List:

Basic Servers	
Processor	Intel®Xeon®E3-1225v3 (3.2GHz/ 8MB/84W)
RAM(max upto 4 DIMMS)	1X4GB DDR3
HDD(max upto 4 drives)	1X1TB SATA 8.89cm (3.5) 7.2k RPM
Price	37999


Lenovo. ThinkServer TS150.

IBM Lenovo Think Server TS150 Tower Server HDD Price List:

Part No	Description	Retail Price
4XB0G88760	Lenovo ThinkServer TS150 3.5"1TB 7.2K Enterprise SATA 6Gbps HDD	13099
4XB0G88764	Lenovo ThinkServer TS150 3.5"2TB 7.2K Enterprise SATA 6Gbps HDD	18199
4XB0G88755	ThinkServer 3.5" 1TB 7.2K SATA 6Gbps Hard Drive	7999

HPE. ProLiant ML350 Gen 10

Electronics > Computers & Accessories > Computers & Tablets > Desktops > Towers



2 videos

HPE ProLiant ML350 Gen10 Tower Server with one Intel Xeon 5218 Gold Processor, 32 GB Memory, and 8 Small Form Factor (SFF) Drive Bays

Visit the Hewlett Packard Enterprise Store

★★★★★ 5 ratings | 4 answered questions

Price: \$6,769.53

Size: ML350 Gen10 5218 1P 32GB-R P408i-a 85FF ...

Brand	Hewlett Packard Enterprise
CPU	Intel
Manufacturer	
CPU Model	Intel Xeon
CPU Speed	2.3 GHz
Processor Count	1

About this item

- Supports the additional 2nd generation Intel Xeon Scalable Processor offerings delivering exceptional customer value with increased performance and industry leading frequency.
- Supports mixed LFF and SFF drive cages within the same server for tiered storage, offering the flexibility to mix drive types for cost and capacity size considerations.
- Available regionally, SMB offers that are aggressively priced.
- HPE ProLiant ML350 Gen10 server supports up to two Intel Xeon Scalable processors, starting from Bronze through Platinum, 4

\$6,769.53

\$574.98 delivery April 19 - May 9. Details

Deliver to Ghana

Only 7 left in stock - order soon.

Qty: 1

Add to Cart

Buy Now

Secure transaction

Ships from US Market Supplies

Sold by US Market Supplies

Return policy: Eligible for Return, Refund or Replacement.


Add an Accessory:

- ☐ Microsoft 365 Family | Premium Office Apps | Up... \$89.99
- ☐ Save \$30 at checkout | Adobe Acrobat Pro DC s... \$178.88
- ☐ Save 68% on McAfee Total Protection 2 Year \$21.99

Fujitsu. Primergy TX1310 M1

HPE ProLiant ML30 Gen10 Xeon E-2224 - 3.4GHz 16GB No HDD - Tower Server - P16930-421

Quickfind code: 1466976



2 videos

You save: £197

£1064.97

or £36.39 a month with PayPal Credit

Add to Basket »

✓ In stock, Order within 3 hrs, 49 mins, 58 secs for delivery tomorrow

✓ FREE Delivery to most of the UK

✓ Collect from Elland today or Collect from Castle Donington on 1st Apr

Why buy me

- Processor - Intel
- RAM - 16GB
- Raid Level - 0,1,5,10

More Info » Tech Spec »

Valid promotions & discounts

Ways to pay

hp HEWLETT PACKARD


HP. ProLiant Microserver Gen8

HPE ProLiant MicroServer Gen8 is a small, quiet, and stylishly designed server that is ideal for micro and small businesses looking to build their first IT server environment.

About 66,000 results (0.97 seconds)

\$449

The HP ProLiant MicroServer Gen8 is available worldwide immediately for a starting price of **\$449**. 3 Oct 2014



<https://www.storagereview.com> > Enterprise

HP ProLiant MicroServer Gen8 Review - StorageReview.com

Was this useful? ☒ Yes ☐ No

About Featured Snippets

Lenovo. ThinkServer TS460

» Data

Lenovo ThinkServer TS460 - tower
- Xeon E3-1240V5 3.5 GHz - 8 GB



Price:
\$1,326.99

Availability: **Call for Availability**

Mfr #: 70TT000QUX
UNSPSC #: 43211501
Item #: 004689505

[Add to Shopping List](#)

1

▲▼

Add to Cart

Need Help? Contact your Zones Account Manager or call 800.408.9663

HP. ProLiant ML350 G9 5U

Electronics > Computers & Accessories > Servers



Roll over image to zoom in

HP 776977-S01 ProLiant ML350 G9 5U Tower Server - 1 x Intel Xeon E5-2620 v3 Hexa-core (6 Core) 2.40 GHz - 2 Processor Support - 8 GB Standard DDR4 SDRAM Maximum RAM - 12Gb/s SAS RAID Supported, Serial ATA Controller - Gigabit Ethernet x 500 W - Matrox G200 Graphic C

Visit the HP Store
★★★★★ 1 rating | 4 answered questions

Price: \$2,100.00

In Stock.

Brand	HP
Hardware Interface	Ethernet
Connectivity Technology	Ethernet
Item Weight	89 Pounds

About this item

- The ML350 Gen9 is the 2P premium server which delivers a class-leading combination of performance, availability, expandability, manageability, reliability and serviceability making it the choice for r

Note: Products with electrical plugs are designed for use in the US. Outlets and voltage differ internationally and this product may require an adapter or converter for use in your destination. Please check compatibility before purchasing.

"You don't build a business, you build people, then people build the business."
-Zig Ziglar



Project Implementation Approval

Project summary and approval

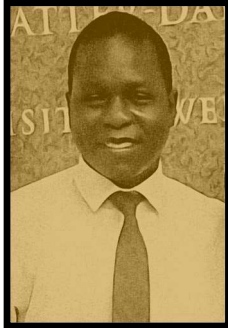
The company's environment is located in a suitable spot for business as many customers strangers visiting the market location would positively impact the organization's efforts to get clients quickly. This exercise's project summary clarifies the purpose as the implementation of server integrated environment would bring to PromisedLand as the essence of this exercise is to showcase the importance of a server to a business organization. Furthermore, there is the shortcoming of server in as much it has to do with system security of protections. The above documents would have to be revisited due to their impacts on security, storage, and uncomplicated business workflow. Attach with this documentation is a summary of video records that show the implemented server on a virtual machine.

With all the precautions in mind, your approval would need to implement the server for PromisedLand at the Hukilau Marketplace at 55-370 Kamehameha Hwy, Laie, HI. 9676. Kindly append your signature for the approval of this project. Thanks for taking the time and effort to go through the proposal.

.....
Date and Signature

Head of Operations

Contact Information



Name

David Odediran

Email

david174@PL.com

Company Details

PromisedLand

55-370 Kamehameha Hwy, Laie, HI. 96762

Tel +233545666550

Website

PL.com

