Deenice Hardware Plan

Hardware Requirements and Quality Assurance

Wendy Liao, Alexander Barstow, Matthew Brady

Updated: Friday, October 9, 2020

Deenice Hardware Plan

Date: Friday, October 9, 2020

Contents

[Hardware Requirements 3](#_Toc53162813)

[Back Up Plan, Storage and Contingency 5](#_Toc53162814)

[Introduction: 5](#_Toc53162815)

[Data Backup Plan and storage 5](#_Toc53162816)

[Testing 8](#_Toc53162817)

[Frequency of testing 8](#_Toc53162818)

[Monitoring and Tools 8](#_Toc53162819)

[Firewall 9](#_Toc53162820)

# Hardware Requirements

What the client might need today is not what the client might need tomorrow, we want to ensure that we are leaving space for more storage, have high enough RAM to run any future processes and ensuring that the CPU is of the highest quality so it does not become out of date. We want to ensure our services and applications can be easily expanded to meet demand.

Notes: These are our basic needs for the hardware plan:

**Based on the information above and the analysis of the services that are required to install, we would recommend:**

|  |  |  |
| --- | --- | --- |
| Items | Minimum requirement | Recommended |
| CPU — limit of CPU that can be used by all replicated VMs of a tenant subscribed to a hardware plan (amount of CPU on the tenant cloud host). | Minimum requirement: 6 core 1.6 GHz CPU | Recommended: 8 core 2.0 GHz CPU |
| Storage — a quota on a datastore (for VMware hardware plans) or a volume (for Hyper-V hardware plans) that a tenant can utilize for storing replicated VMs data | Minimum requirement: 500 GB space | Recommended: 4 TB of storage |
| Memory — limit of RAM that can be used by all replicated VMs of a tenant subscribed to a hardware plan (by all tenant VMs on the cloud host). | Minimum requirement: 7 GB | Recommended: 32 GB |

More detailed breakdown and research:

|  |  |  |  |
| --- | --- | --- | --- |
| Items needed | CPU power needed | Storage | Memory (RAM) |
| 2 vSphere hosts  ESXi 6.7 | At least two CPU cores  supports 64-bit x86  requires the NX/XD bit to be enabled for the CPU in the BIOS. | requires a boot device that is a minimum of 1 GB.  When booting from a local disk, SAN or iSCSI LUN, a 5.2-GB disk is required to allow for the creation of the VMFS volume and a 4-GB scratch partition on the boot device.  Although a 1GB USB or SD device  suffices for a minimal installation, you should use a 4GB or larger device. The extra space is used for an expanded coredump partition on the USB/SD device. Use a high-quality USB flash drive of 16 GB or larger so that the extra flash cells can prolong the life of the boot media, but high-quality drives of 4 GB or larger are sufficient to hold the extended coredump partition | 4 GB of physical RAM.  It is recommended to provide at least 8 GB of RAM |
| Minimum needed: 2 CPU cores | Minimum needed: 4GB | Minimum needed: 4GB  Recommended: 8GB |
| HTTP | Combined Web & Database Server (recommended)  1,6 GHz CPU  4 x 1,6 GHz CPU | 1x 40 GB of free space or more is recommended for the webshop data (non-system drive is preferred) 1x 40 GB of free space or more is recommended for the software that is listed in the software requirements (system drive) | Combined Web & Database Server  7GB RAM |
| Minimum needed: 1,6 GHz CPU  Recommended: 4 x 1,6 GHz CPU | Recommended: 4GB | Minimum needed: 1,75 GB RAM  Recommended:7 GB RAM |
| DNS | 400 MHz or better. | 10 MB + Windows and .NET Framework requirements. | 64 MB + Windows and .NET Framework requirements. |
| Minimum: 400MHz | Minimum: 10 MB | Minimum: 64MB |
| Active Directory (not LDAP) | 1.4Ghz 64-bit processor or faster. | 32GB of disk space or greater. | 512MB of RAM or greater. |
| Minimum: 1 1.4GHz 64-bit | Minimum: 32 GB | Minimum: 512 MB RAM |
| iSCSI Target and Initiator | six to eight CPU cores | 24x15k-RPM disks in a RAID (for 256 computers)  format the partitions with NTFS  at least 1TB | 16 GB RAM |
| Minimum: 6 CPU cores  Recommended: 8 CPU cores | Minimum: 24  Recommend: 1TB | Minimum: 6GB RAM  Recommended: 16GB |
| File Server (SMB, NFS, or other) | 2.0GHz CPU with dual-core processor minimum (Recommended: Quad-core i5 processor or better) | At least 100 GB disk allocation | 4GB of RAM minimum (Recommended: 8GB or more) |
| Minimum: 2 CPU cores, 2GHz  Recommend: i5 or higher | Minimum: 100 GB | Minimum: 4 GB  Recommended: 8 GB |
| Veeam Community Edition( Enterprise Backup) | x86-64 processor (4 cores recommended). | GB1 for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data).  Additional free disk space for Instant VM Recovery cache folder (non-persistent data, at least 10 GB recommended). | 4 GB RAM plus 500 MB RAM for each concurrent job |
| Minimum: 4 cores | Minimum: 10 GB  Recommended: 15GB | Minimum: 4GB |
| Windows Admin Center (WAC) | 1.4 GHz 64-bit processor | The following are the estimated minimum disk space requirements for the system partition.  Minimum: 32 GB | 512 MB (2 GB for Server with Desktop Experience installation option) |
| 1 core, 1.4 GHz | Minimum: 32GB | Minimum: 2GB |
| Spiceworks | Intel i5 or better | Solid-state drive or other high-availability disk backend  20 GB hard drive or higher | 6-8 GB available |
| I5 GHz | Minimum: 20 GB | Minimum 6 GB  Recommended: 8 GB |
| Linux OS | 2 GHz dual core processor. | 25 GB of hard-drive space (or USB stick, memory card or external drive but see LiveCD for an alternative approach) | 4 GiB RAM (system memory) |
| Minimum: 2 x 2GHz | Minimum: 25GB | Recommended: 4GB |
| Windows OS | 1.4 GHz 64-bit processor. | Disk Space - 32 GB. | RAM - 512 MB. |
| Minimum: 1.4 GHz | Minimum: 32 GB | Minimum: 512 Mb |
| Minimum requirements: | 6 CPU cores  Recommended: 8 CPU cores, running 2GHz | Minimum: 500 GB (ideally for space)  Recommended: for system: 1.5 TB | Minimum: 7GB  Recommended: 16 GB |

# Back Up Plan, Storage and Contingency

Introduction:

While a contingency plan defines how the we will operate during an attack, we will also need to take steps to minimize potential loss of data and other information after an attack. We must have an effective backup plan in place to rapidly restore service following a cyberattack.

## Data Backup Plan and storage

A back up is a separate copy of the important files, applications and data so if something happens to our system, our information is completely safe and accessible.

### Backup

* Systems need to be redundant and load-balanced
* Data should be mirrored so that if something happens, it can be backed up
* Recommend: RAID 10: Disk striping with mirroring
  + RAID 10 requires a minimum of four disks in the array. It stripes across disks for higher performance, and mirrors for redundancy. In a four-drive array, the system stripes data to two of the disks. The remaining two disks mirror the striped disks, each one storing half of the data.
* Media:
  + Data should be backed up on 3 different systems, including being backed up on HDD/SSDs physically, magnetic discs, on the cloud, and in two different locations. Tape backups and on the cloud digitally.
* Regular full backups are done:
  + Once a week, on Friday nights at 1:00am.
* Differential back up is done:
  + Twice a week, Wednesdays and Sundays, at 1:00am (during time when network may not be in use or may have lower usage)
  + This is slower than an incremental backup, but has a faster recovery time. This backs up data since the last full backup. This is much faster than a full backup.
* Will have automatic failover:
  + Automatic failover is when a hard drive fails and a backup hard drive automatically takes over the function without delay or interruption in service.
* Will have server clustering:
  + Server clustering: Server clustering is when more than one server is used to increase the service to the user

Note, we want to ensure that we have:

* 3 copies of our data
* 2 local copies on different storage types
* 1 backup off-site

### Contingency Plan

Purpose: The purpose of this Continuity Plan is to assure that, in the event of a disaster, equipment failure or software failure, critical business processes will continue**.**

**In general, there are 4 phases:**

1. Disaster (Initial Response)
2. Recovery (and preparation for backup site if necessary)
3. Restoration (Backup site fully operational, Restoration and return to permanent facility)
4. Evaluation (To evaluate the disaster and plan for future)
   1. Response (in the case of disaster):

* Notify the client’s incident response team or main technical points of contact, affected managers and personnel
  + Ensure that there is an incident response team with the client
  + Ensure that there are regular reviews and updates to the contingency plan to accommodate updates and changes in technology
* Two Uninterruptible Power Supply (UPS) are implemented to prevent data loss. Each battery should have enough power for at least 8 hours, or until someone can get in to fix it.
* Run breach containment procedure
  + This could include (depending on the level of breach) shutting down any systems that are not vital for the operation, including phone or VPN or specific users’ email access
  1. Recovery:
* Assess the availability and capability of personnel
* Assess the operational status and damage to hardware, software, compute rooms, network infrastructure, network services, servers, applications and data
* Execute the recovery plan based on the damage assessment, including:
  + restoring vital network links, infrastructure, servers and applications
  + Reconfiguring any networks and servers as needed.
  + Restoring applications and data from backup and any secondary services
* Ensure that backups can be brought back up and running within four hours
  1. Restoration
* Evaluate all items to ensure that everything has been brought back to pre-disaster
  1. Evaluation
* Evaluate the risk of the breach, evaluate the risks, including what harm might have been done and who was affected
* Conduct an incident review of the incident to help prepare for future breaches and have policies in place to learn for the future
* Make any required patches or updates

### Preventative measures:

* Ensure there is a user awareness training in areas such as incident handling, disaster recovery, securing data, phishing and safety online.
* Ensure that the contingency plan is distributed to the correct people
* The plan should be reviewed with all employees at least annually
* Plans should be created for things such as water damage, electrical failure, sabotage, fires, natural disasters or hardware failure

# Testing

To ensure that all services and devices are working as intended we will be following the testing plan laid out in testplan.xlsx. This spreadsheet contains a set of generic tests applicable to all services and, a more specific set of tests for each service.

## Frequency of testing

Each test will be done a minimum of three times. The first two instances will be directly after initial configuration, once each by the acting administrator and a peer. All tests will be run a final time between October 19th and November 29th (Item 26 in the project plan) to ensure proper functionality before the project demonstration. If the team encounters an error at any time, testing will restart and require two new tests before the service is considered operational again.

# Monitoring and Tools

For monitoring our network, there are several easily accessible software which can be used on our jumpbox.

We already plan to deploy Spiceworks which has monitoring capabilities for Windows environments through WMI, allow for the restarting of services remotely and, observing network alerts. It also has an automation feature allowing us to create custom alert for our machines.  
  
At a more basic level, key standbys like Wireshark and nmap can be used to monitor network traffic and provide a snapshot of open ports and the types of protocols which used in our network. We plan to leverage scripts using the aforementioned commands to automate some network logging and catch network problems.

Networking tools which will allow us to use the information we gather from monitoring tools will then be employed. Should our monitoring through Spiceworks, Wireshark and nmap show a loss of snmp connectivity, we can use Putty’s ssh and telnet capabilities (mindful of the firewall, see below) and ping to test the level of connectivity still available.

Alongside all of this, the machines are also managed through vSphere, allowing access to the servers should all other connectivity fail. Down interfaces on the servers can be brought back up, and service in general should not be affected as the network has been designed with redundancy and fault tolerance in mind.

# Firewall

In order to ensure the security of the network and of the client’s information, it is imperative to create a strong set of rules for our firewall. Best practices for a firewall demand we deny all traffic other than allowing SSH (port 22), HTTP (port 80) and should we choose to use it, SMTP (port 25)

After that, we make the various devices in our network exceptions to the firewall’s denial of traffic, listing our traffic network (172.20.57.0/16), management network (172.30.57.0/16), ESXi network (172.40.57.0/16) and our iSCSI network (172.50.57.0/16) so as not to block traffic from our own network. Of key importance, the jumpbox must not be allowed free access to our network without precaution to prevent outside attacks on the network from coming from the internet or another public network through the jumpbox.