All Others Stuff

- Veeam Duplicate UUID
- WordPress - Setup WordPress
- VMWare - Install Windows 11 on vCenter 8 without TMP 2.0
- File Transfer - Using FTP LFTP commands
- File Transfer - WPUT
- File Transfer - CURL
- Asus - OpenVPN Site to Site or Point to Point
- MarkDown - Guide .md
- Certificate - PKCS12
- DELL - XPS Killer Wifi
- Caffeine Hack - Got caught with Caffeine installed
- Synology - Host Unifi for FREE on Synology NAS
- Concrete - Dry Pour Schedule
- Synology - Upgrade 1515+ to 1517+
- PiHole - Configuration
- ESXi - UPS Nut Installation
- Synology - Flash uboot ROM
- HPE - iLO4 Reflash after Not Responsive 380p Gen8
- VMWare - Copy and Paste from Console to VM
- MailServer - Test SMTP
- ImageMagick - Install on Redhat 9 from Source
- IPCamera - Different Configs
- HPE - ProLiant DL380p Gen8 GPU Install
- Dell - Hard Drive Capacity Difference Between Drives

Synology - Bag of Tricks

sudo -i

ip link set eth1 down

My DS118 idles at 24% after disabling all the junk.

//run once as root to disable services *you* don't need

synopkg stop pkgctl-SynoFinder
synopkg uninstall SynoFinder
synopkg stop pkgctl-ActiveInsight
synopkg uninstall ActiveInsight
synopkg stop pkgctl-ScsiTarget
synopkg uninstall ScsiTarget
synopkg stop pkgctl-SecureSignIn
synopkg uninstall SecureSignIn
synopkg stop pkgctl-Python2
synopkg uninstall Python2

//root task disable thumbnails every boot if you're not indexing

cd /var/packages/FileStation/target/etc/conf/
mv thumbd.conf thumbd.conf.bak

Downgrade Synology DSM 7 (to 6)

I thought I would take the time to share how I downgraded my Synonlogy 1019+ from DSM version 7 to version 6.2.x. The reason for this was that after upgrading, I was no longer able to use Syncthing, and I really needed this working ON the NAS itself. After the upgrade to DSM 7, Plex broke initially as well, but I have a tip at the end of how I fixed this (if you are keeping DSM 7).

1. BACKUP YOUR CURRENT CONFIGURATION!!!!!!

1. Get Putty. If you have a Mac, you can use Terminal for the first part, but if you've upgraded to the most recent version of OSX, you won't get Telnet in ZSH. So yeah, just use Putty.
2. In your Control Panel (on the NAS), enable Telnet and SSH.
3. Login to your NAS via SSH (using Putty or Terminal), using your admin account and password.
4. Do the following: sudo vi /etc.defaults/VERSION

[ENTER]

when prompted, enter your password

5.Once in the VI editor, press the "i" (eye) key to be able to insert data. Overwrite all content, and replace it with the following:

majorversion="6" minorversion="2" productversion="6.2.3" buildphase="GM" buildnumber="25426" smallfixnumber="0" builddate="2020/07/01" buildtime="06:24:39"

1. To save, do the following:

[ESC]

:wq!

[ENTER]

sudo reboot [ENTER] (or reboot from the web interface)

1. Once the NAS reboots, use the Synology Assistant to find it. Follow the prompts to reinstall DSM.

1. At the screen that prompts you to choose the version of DSM to install, choose the Manual option, and click the link beside it and download version 6. Download the DSM version you want.

1. Continue the installation process by browsing to, and selecting the DSM version 6 file you just downloaded. As the process continues, you will be met with an error. At this point STOP, the Telnet port will be opened. Do the following:

10. Using Putty, choose the Telnet option, enter the IP address of your NAS, ensure that port 23 is chosen, and connect.

11. Enter "root" as the user, and the password of "101-0101" (without the quotes).

12. Repeat Step 4, except you should not enter "sudo" since you are already root. Repeat Step 5.

13. It took me quite some time to figure out this one issue. When I would go to save the edited file, I kept getting an error, and it did not make sense. Eventually, I figured it out. Repeat step 6, except don't do the combination write and quit (:wq!) command as before. I had to do a write first, then a quit. As below:

Assuming you entered the information from Step 12...

[ESC]

:q [ENTER][ENTER]

:w [ENTER][ENTER]

14. Go back to your browser, and continue the installation of DSM 6.

Good luck.

Bonus Tip if you keep DSM 7:

I removed the original steps to fix Plex if you KEEP DSM 7. According to the user below, simply follow Plex’s instructions by downloading the latest version of Plex and using that. Thank you. I thought I had to choose repair first, then I “fixed” my issue, but apparently it was not necessary.

VMWare - Delete inaccessible datastore

Rename the store

Use the web client to rename each store and a DEL in front of the name

Access the shell of the appliance server and then the database

```
VMware vCenter Server 8.0.2.00300

Type: vCenter Server with an embedded Platform Services Controller

Connected to service
* List APIs: "help api list"
* List Plugins: "help pi list"
* Launch BASH: "shell"

Command> shell
Shell access is granted to root
root@vcenter80 [ ~ ]#
```

```
shell;/opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres
```

View the stores

This will give you the ID that is needed to clean up

```
SELECT * FROM vpx_entity;
```

Delete the store

This is the delete for cleaning up the inaccessible datastore

```
DELETE FROM vpx_ds_assignment WHERE ds_id=1015;
DELETE FROM vpx_datastore WHERE id=1015;
DELETE FROM vpx_vm_ds_space WHERE ds_id=1015;
DELETE from vpx_entity where id=1015;
```

Change the ID and then run the following

```
DELETE FROM vpx_ds_assignment WHERE ds_id=5015;DELETE FROM vpx_datastore WHERE id=5015;DELETE FROM vpx_vm_ds_space WHERE ds_id=5015;DELETE from vpx_entity where id=5015;
```

Restart the services

```
\q;service-control --stop --all && service-control --start --all
```

Proper Active Directory Time Sync Methods

Network Time Protocol (NTP) is a long-standing standard for computers to synchronize time between systems. NTP can be used to ensure that all synchronized computer clocks maintain the same time within a very small margin, usually measured in milliseconds. While making sure all your devices report the correct time is convenient in and of itself, ensuring proper time settings is paramount to security in ways you might not expect. Here are a few security-related items that rely on accurate time settings to work correctly:

- Certificate verification
- Kerberos authentication
- Log integrity
- One-time password (OTP) two-factor authentication

Generally, the best practice setup involves creating a trusted time source for internal clients to use as a reference to sync against. This internal time source in turn syncs against a trusted external time source. Following the trail of time syncing, we would expect time to sync from the trusted external source to the trusted local source to all other clients as seen in Figure 1. You may consider having the Active Directory domain controller (DCs) sync to an external time source independently rather than use a single trusted internal source, but this would cause additional overhead and problems such as clock drift that you may not realize until it becomes an issue.

Figure 1 – Proper syncing from an external time source to a trusted internal source

image.png
Image not found or type unknown

Take an example where the external time source is no longer available. Your clocks will slowly begin to drift until they eventually desynchronize, causing issues such as failed Kerberos authentication. The worst-case scenario for a single trusted time source is that the entire environment “fails together” but clients still have accurate time relative to each other, allowing your critical services to keep moving. All internal clocks would have the same time even if synchronization to the external source were to stop working.

Because time services are a necessity for any network, there are many trusted sources that offer public NTP servers for clients and other networks to sync against. While not nearly an exhaustive list, the following table lists a few example sources.

Provider	URL

Google	http://time.google.com
CloudFlare	time.cloudflare.com
Microsoft	time.windows.com
Apple	time.apple.com
NIST	time.nist.gov
NTP Project	pool.ntp.org

Microsoft’s Recommendations

Active Directory (AD) has a built-in NTP server configured on DCs. Modern DCs leverage NTP with backward compatibility support for Simple Network Time Protocol (SNTP) used in some older Windows environments such as Windows 2000. In most situations where Active Directory Domain Services (AD DS) is already installed, a Domain Controller makes a great candidate for internal time servers that can support both NTP and SNTP. There are usually multiple DCs in any given environment, so the role of determining the base time for all other DCs and by extension all other clients is the responsibility of the DC with the Primary Domain Controller Emulator (PDCe) Flexible Single-Master Operation (FSMO) role in the forest root domain. Figure 2 shows an example configuration using DCs as time servers.

Figure 2 – Example time sync configuration for a single AD domain

image.png
Image not found or type unknown

While the PDC emulator will likely be using the standard NTP protocol to sync from an external source, all other DCs, member servers, and client computers joined to the domain will typically be configured to forego use of the NTP protocol for the Microsoft-specific NT5DS time synchronization method. Typically, any client joined to the domain should be configured to use NT5DS to synchronize time through AD automatically. In most situations, no actual client configuration should be required unless an existing configuration that uses NTP needs to be removed.

Multi-Domain Forest NTP Considerations

Time synchronizations for forests that have multiple domains don’t all sync directly with the parent domain PDCe DCs. In a situation where one or more child domains exist, time synchronization can be determined using the following table.

Domain	Device Type	Syncs Time From
Parent	PDCe DC	External time source
Parent	Non-PDCe DC	Parent domain PDCe DC
Parent	Domain-joined client	Parent domain DC
Child	PDCe DC	Any parent domain DC
Child	DC	Any child domain DC
Child	Domain-joined client	Child domain DC

Note: this table assumes the CrossSiteSync flag is set to the Microsoft default of 2; other configurations are possible and will be elaborated on in a future blog post

Configuring a Robust Internal Time Syncing Infrastructure

While it's trivial to configure external NTP synchronization from the PDCe, it becomes another item to manage and configure in the event of transferring FSMO roles. A more robust solution that would allow for external NTP configurations to be transferred along with the PDC emulator role would be ideal. To this end, the following configuration items are recommended:

- Create a Group Policy Windows Management Instrumentation (WMI) filter to target the PDCe role holder.
- Create a Group Policy Object (GPO) to allow the PDCe to sync time from a trusted external source, apply the WMI filter you previously created, and link the GPO to the default Domain Controllers organizational unit (OU).

This means that if the PDCe role is transferred from one Windows server to another, Group Policy will enforce external time syncing on the DC with the newly acquired PDCe role. Once the policy for the PDCe is unlinked due to role change, the old PDCe returns to the normal NT5DS synchronization—allowing it to gather time from the new PDCe rather than the originally configured external time source.

Requirements for Configuration

- The DC(s) that may be serving as PDCe are allowed to access the configured external trusted time server using the NTP protocol [UDP Port 123].

- The DCs not serving as the PDCe are allowed to access the PDCe using the NT5DS protocol [UDP Port 123].
- Clients can reach the DCs serving as NTP servers using both the NTP and NT5DS protocol [UDP Port 123].

PDCe DC Role Filter Configuration

The first required step is to create the WMI filter that will be used to ensure only the PDCe is allowed to sync from an external time source. This can be configured from the Microsoft Management Console (MMC) Active Directory Group Policy Management snap-in, as Figure 3 shows.

1. Right-click the **WMI Filters** folder and right-click **New**
2. Give the new filter a meaningful name, for example **PDCe DC Role Filter**
3. Give the new filter a meaningful description such as "**This filter will search for a computer with the PDCe FSMO Role [DomainRole 5]**"
4. Create a new query by clicking **Add**
5. Leave the **Namespace** field at the default value of **root\CIMv2**
6. Enter the following text for the **Query** value: **Select * from Win32_ComputerSystem where DomainRole = 5**

Figure 3 – Example role filter to target only the PDCeNote: this query will specifically look for the DomainRole value of 5 which is only used by the DC with the PDCe FSMO role

image.png
Image not found or type unknown

PDCe NTP Configuration GPO Creation

The next step is to create a GPO that will configure the PDCe to sync time from an external source. This can be configured from the MMC **Active Directory Group Policy Management** snap-in.

1. Right-click the **Group Policy Objects** folder and click **New**
2. Give the new GPO a meaningful name such as **Configure PDCe Time Server**
3. Select **Configure PDCE Time Server GPO** and set the **WMI Filtering** filter to **PDCE DC Role Filter**
4. Edit the **Configure PDCE Time Server GPO** and navigate to: Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time Providers
5. Edit the **Configure Windows NTP Client** setting and set the following values:

Status	**Enabled**
NtpServer	http://us.pool.ntp.org **,0x9** http://1.us.pool.ntp.org **,0x9 2.us.pool.ntp.org,0x9** http://3.us.pool.ntp.org **,0x9;**
Type	NTP
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	3600
EventLogFlags	3

Note: You may choose different external time servers based on your location and needs; these values are only given as an example but will work.

1. Edit the **Enable Windows NTP Client** setting and set the following value:
   Status: **Enabled**
2. Edit the **Enable Windows NTP Server** setting and set the following value:
   Status: **Enabled**
3. Exit the **Configure PDCE Time Server** Group Policy window
4. Right-click the **Domain Controllers** OU and select **Link an Existing GPO**
5. Select **Configure PDCE Time Server** and click **OK**

Testing NTP Configuration on the PDCe

1. Log on to the **PDCe** DC and open an administrative CMD prompt
2. Perform a Group Policy update by entering the following command: **gpupdate /force**
3. Confirm that Group Policy has been updated successfully
4. Check the NTP client configuration by entering the following command: **w32tm /query /status**

The output should confirm that the source is one of the external time servers configured in the GPO, as seen in Figure 4.

Figure 4 – The PDCe is correctly syncing from an external source

image.png
Image not found or type unknown

Testing NTP Configuration on a Non-PDCe DC or Client

1. Log on to a non-PDCe DC and open an administrative CMD prompt
2. Perform a Group Policy update by entering the following command: **gpupdate /force**
3. Confirm that Group Policy has been updated successfully
4. Check the NTP client configuration by entering the following command: **w32tm /query /status**

The output should confirm that the source is the PDCe or DC, as seen in Figure 5.

Figure 5 – The DC is correctly syncing time from the PDCe

image.png
Image not found or type unknown

Final Considerations

Time synchronization is an important yet sometimes overlooked part of security. Luckily, the tools offered through AD allow for a relatively simple time synchronization configuration that proves to be robust and survivable even through FSMO role changes. It may also be worth investigating other NTP configurations, such as configuring DHCP Option #42 to automatically configure NTP sources on your network for non-domain-joined devices.

from: https://www.ravenswoodtechnology.com/in-sync-proper-active-directory-time-sync-methods/

Synology - Backup from Linux

Introduction

This is to setup a hourly MySQL backups and also a full system backup once a week.

Synology Configuration

NFS Configuration

You will need to go to the Control Panel → File Services under the NFS section and turn it on

image.png
Image not found or type unknown

Then hit APPY

Then go to Shared Folder to setup the share you would like to use for the backups

image.png
Image not found or type unknown

Linux Configuration

Now login to the Linux server to setup FSTAB to allow the NFS link to work

Edit the “/etc/fstab“

```
#Custom
bigberta.onling.com:/volume1/Backups /mnt/backups nfs auto,defaults 0 0
```

Create the directory for the mount

```
mkdir -p /mnt/backups
```

After the mount the new NFS drive

```
mount -a -v
systemctl daemon-reload
```

To force kill the new mount

```
umount -l /mnt/backups
```

Linux - FTP Using Bash

Example of simple bash script ftp client

This script first defines variables such as hostname of the ftp server, username and password and then it creates an ftp session and uploads the specified file into your selected directory:

```
#!/bin/bash

ftp_site=127.0.0.1
username=ftpuser
passwd=pass

PS3='Select a destination directory: '

# bash select
select path in "." "/test" "public_html/myblog/" "backup/images/"
do
ftp -n $ftp_site<<EOF
quote USER $username
quote PASS $passwd
binary
cd $path
put $1
quit
EOF
break
done
```

Be sure to edit the `ftp_site`, `username`, and `passwd` variables above. You should also change the paths to whichever directories you most commonly upload your files to.

Executing the script:

```
$ chmod +x ftp_bash_script.sh
$ ./ftp_bash_script.sh file1
```

Example script output:

```
$ ./ftp_bash_script.sh somerandomfile
1) .
2) /test
3) public_html/myblog/
4) backup/images/
Select a destination directory: 2
Connected to 127.0.0.1.
220 (vsFTPd 3.0.5)
331 Please specify the password.
230 Login successful.
200 Switching to Binary mode.
250 Directory successfully changed.
local: somerandomfile remote: somerandomfile
229 Entering Extended Passive Mode (|||10078|)
150 Ok to send data.
    0        0.00 KiB/s
226 Transfer complete.
221 Goodbye.
```

XWiki - Install

This is to create a installation of XWiki on a installation of Rocky Linux already installed

Configuration

Linux configuration

Disable selinux

Run the following or you can modify the file here, “/etc/sysconfig/selinux”. If you modify the file make sure you still run the “setenforce 0” or just simply reboot after modification.

```
setenforce 0
sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
```

Disable firewall

```
systemctl disable firewalld.service
```

Epel Release

```
dnf install epel-release -y
```

After Epel install

```
dnf upgrade -y
```

Server Software Configuration

Install MySQL on the server

Install Java

```
dnf install java-11-openjdk -y
dnf install java-11-openjdk-devel -y
```

Verify the Viserion after install

```
java -version
```

Results

```
openjdk version "11.0.24" 2024-07-16 LTS
OpenJDK Runtime Environment (Red_Hat-11.0.24.0.8-2) (build 11.0.24+8-LTS)
OpenJDK 64-Bit Server VM (Red_Hat-11.0.24.0.8-2) (build 11.0.24+8-LTS, mixed mode, sharing)
```

Install MariaDB

Install the server

```
sudo dnf install mariadb-server -y
```

Modify the my.cnf server file

```
sudo vi /etc/my.cnf.d/mariadb-server.cnf
```

Make modifications the file and append under the current settings in the [mysql] section

```
#Custom Entries
performance_schema = ON
tmpdir = /run/mariadb
thread_cache_size = 4
table_open_cache = 16384
table_definition_cache = 8384
sql_mode = ERROR_FOR_DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION

query_cache_type = 0
query_cache_size = 0
query_cache_limit = 128M
query_cache_strip_comments = 1

tmp_table_size = 512M
max_heap_table_size = 512M

max_connections = 512
max_allowed_packet = 24M
```

```
sort_buffer_size = 24M
join_buffer_size = 48M

innodb_buffer_pool_size = 4G
innodb_buffer_pool_instances = 4
innodb_use_native_aio = 1
innodb_flush_log_at_trx_commit = 0
innodb_file_per_table
innodb_log_file_size = 512M

#Optional config if using transaction log.
log_bin = /var/log/mariadb/mariadb.log
expire_logs_days = 2
```

Reload for changes

```
sudo systemctl daemon-reload
```

Start and enable on boot

```
systemctl enable --now mariadb.service
```

Add the XWiki user to access the database

```
mysql
create database xwiki default character set utf8mb4 collate utf8mb4_bin;
grant all privileges on xwiki.* to 'xwiki'@'localhost' identified by 'xwiki_password';
grant all privileges on xwiki.* to 'xwiki'@'%' identified by 'xwiki_password';
FLUSH PRIVILEGES;
exit;
```

Tomcat Configuration

Verify which version you want to install, we will be using “v9.0.63”

```
http://dlcdn.apache.org/tomcat/tomcat-9
```

Create folder for Tomcat

```
sudo mkdir /opt/tomcat
sudo cd /opt/tomcat
```

Replace the version within the following link

```
wget https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.93/bin/apache-tomcat-9.0.93.tar.gz
```

Extract the file you downloaded in you current folder

```
sudo tar xvf apache-tomcat-*.tar.gz -C /opt/tomcat --strip-components=1
```

Create the tomcat user

```
sudo groupadd tomcat
sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat
```

Change the permissions on the tomcat folder

```
sudo chown -R tomcat: /opt/tomcat
```

Configuring Systemd Service

```
sudo vi /etc/systemd/system/tomcat.service
```

Add the following content to the file

```
[Unit]
Description=Tomcat 9 servlet container
After=network.target

[Service]
Type=forking

User=tomcat
Group=tomcat

Environment="JAVA_HOME=/usr/lib/jvm/jre"
Environment="CATALINA_PID=/opt/tomcat/temp/tomcat.pid"
Environment="CATALINA_HOME=/opt/tomcat"
Environment="CATALINA_BASE=/opt/tomcat"
Environment="CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC"
```

```
Environment="JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom"

ExecStart=/opt/tomcat/bin/startup.sh
ExecStop=/opt/tomcat/bin/shutdown.sh

[Install]
WantedBy=multi-user.target
```

Enable and start the Tomcat service:

```
sudo systemctl daemon-reload
sudo systemctl enable tomcat
sudo systemctl start tomcat
```

Adjusting the Firewall and you did not run the firewall disabling command above, allow traffic to Tomcat's default port 8080

```
sudo firewall-cmd --permanent --zone=public --add-port=8080/tcp
sudo firewall-cmd --reload
```

Securing Tomcat

Edit the `web.xml` file to disable directory listing and add security constraints to the manager and host-manager applications. It's also advisable to change the default shutdown port and command in `server.xml`.

Add access from another host if needed

```
vi /opt/tomcat/webapps/manager/META-INF/context.xml
```

Add the IP or IPs you are accessing from to allow access to the main tomcat page. you will need to change this entry from this “allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1” />" to something like this

```
allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1|192.168.253.100|192.168.252.2" />
```

Configure XWiki

Download the war file

```
cd /opt/tomcat/webapps
wget -O wiki.war https://nexus.xwiki.org/nexus/content/groups/public/org/xwiki/platform/xwiki-platform-distribution-war/15.10.11/xwiki-platform-distribution-war-15.10.11.war
systemctl restart tomcat
```

Reverse Proxy

Change for reverse proxy settings

```
sudo vi /opt/tomcat/webapps/wiki/WEB-INF/xwiki.cfg
```

Change the following in the file

To point to a specific domain

```
xwiki.home=http://wiki.sflservicesllc.com
```

Change to use https

```
xwiki.url.protocol=https
```

MySQL Setup

After the Tomcat service is restarted move to the XWiki’s WEB-INF/lib directory and download the MySQL JDBC Driver JAR:

```
su - tomcat
cd /opt/tomcat/webapps/wiki/WEB-INF/lib/
wget https://repo1.maven.org/maven2/mysql/mysql-connector-java/5.1.49/mysql-connector-java-5.1.49.jar
chown tomcat:tomcat mysql-connector-java-5.1.49.jar
```

MariaDB Setup

After the Tomcat service is restarted move to the XWiki’s WEB-INF/lib directory and download the MariaDB JDBC Driver JAR:

```
su - tomcat
cd /opt/tomcat/webapps/wiki/WEB-INF/lib/
wget https://dlm.mariadb.com/3852266/Connectors/java/connector-java-3.4.1/mariadb-java-client-3.4.1.jar
chown tomcat:tomcat mariadb-java-client-3.4.1.jar
```

Open the WEB-INF/hibernate.cfg.xml file and configure XWiki to use MySQL:

```
vi /opt/tomcat/webapps/wiki/WEB-INF/hibernate.cfg.xml
```

Comment out the default hsqldb database section and uncomment and edit the MySQL database section as shown below:

```
<!-- Configuration for the default database.
Comment out this section and uncomment other sections below if you want to use another database.
Note that the database tables will be created automatically if they don't already exist.

If you want the main wiki database to be different than "xwiki" (or the default schema for schema based engines)
you will also have to set the property xwiki.db in xwiki.cfg file
-->
<!--
<property name="connection.url">jdbc:hsqldb:file:${environment.permanentDirectory}/database/xwiki_db;shutdown=true</property>
<property name="connection.username">sa</property>
<property name="connection.password"></property>
<property name="connection.driver_class">org.hsqldb.jdbcDriver</property>
<property name="dialect">org.hibernate.dialect.HSQLDialect</property>

<property name="hibernate.connection.charSet">UTF-8</property>
<property name="hibernate.connection.useUnicode">true</property>
<property name="hibernate.connection.characterEncoding">utf8</property>

<mapping resource="xwiki.hbm.xml"/>
<mapping resource="feeds.hbm.xml"/>
<mapping resource="activitystream.hbm.xml"/>
<mapping resource="instance.hbm.xml"/>
<mapping resource="notification-filter-preferences.hbm.xml"/>
<mapping resource="mailsender.hbm.xml"/>
-->
```

Uncomment wither the MySQL Section or the MariaDB section and change the password

```
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.password">xwiki_password</property>
```

Restart the Tomcat service

```
sudo systemctl restart tomcat
```

Accessing Tomcat

Open your web browser and navigate to the following below. You should see the default Tomcat landing page.

```
http://[your_server_ip]:8080/wiki
```

https://linuxhostsupport.com/blog/how-to-install-xwiki-on-centos-7/

https://reintech.io/blog/installing-configuring-tomcat-rocky-linux-9

Synology - Moving Packages Between Volumes DSM 7.0

1. Stop the application(s) via the Synology package center.
2. Make sure that Telnet/SSH is enabled
3. Login to Synology using SSH and elevate to root.
4. Make sure that the volume you are moving the application(s) to have the following folders:
    1. @appstore
    2. @apphome
    3. @appconf
    4. @apptemp
        1. If they do not you will have to create them in super user mode "*sudo -i*" for all of the following commands
        2. ```
           sudo -i
           cd /volume2
           mkdir /volume2/@appstore
           mkdir /volume2/@apphome
           mkdir /volume2/@appconf
           mkdir /volume2/@apptemp
           ```
5. Find the application that you need to move on the correct value
    1. Use "ls" against */VolumeX/@appstore* to find your package folder name
    2. ```
       cd /volume1/@appstore
       ls -lart
       drwxr-xr-x 15 AudioStation          AudioStation          4096 Oct  6 22:37 AudioStation
       drwxr-xr-x 16 MediaServer           MediaServer           4096 Oct  6 22:40 MediaServer
       drwxr-xr-x  9 iTunesServer          iTunesServer          4096 Oct  6 22:41 iTunesServer
       drwxr-xr-x 23 SurveillanceStation   SurveillanceStation   4096 Jan 24 17:13
       SurveillanceStation
       ```
    3. Use "mv" to move the data between the old and new volume, you may need to create the *@appstore* folder first.
    4. ```
       mv SurveillanceStation /volume2/@appstore/
       ```
       ```

6. Now you will need to adjust Synology and relocate the parameters for the application(s) and where it is now moved to. this is done where the packages configurations live in “*/var/packages*”.
    1.
    ```
    cd /var/packages/SurveillanceStation
    ls -lrt
    lrwxrwxrwx 1 root root    33 Oct  6 22:33 var -> /volume1/@appdata/UniversalViewer
    lrwxrwxrwx 1 root root    33 Oct  6 22:33 tmp -> /volume1/@apptemp/UniversalViewer
    lrwxrwxrwx 1 root root    34 Oct  6 22:33 target -> /volume1/@appstore/UniversalViewer
    lrwxrwxrwx 1 root root    33 Oct  6 22:33 home -> /volume1/@apphome/UniversalViewer
    lrwxrwxrwx 1 root root    33 Oct  6 22:33 etc -> /volume1/@appconf/UniversalViewer
    ```
    2. Now we have to remove the symbolic links and recreate them to point to volume2 using the “*rm*” to remove and the “*ln -s*” to recreate them.
    3.
    ```
    rm var tmp target home etc
    ln -s /volume2/@appdata/UniversalViewer var
    ln -s /volume2/@apptemp/UniversalViewer tmp
    ln -s /volume2/@appstore/UniversalViewer target
    ln -s /volume2/@apphome/UniversalViewer home
    ln -s /volume2/@appconf/UniversalViewer etc
    ```
    4.
7. Repair your application(s) package in the Synology Package Centre.
    1. It will automatically re-download and restart

Veeam Upgrade

https://www.reddit.com/r/Veeam/comments/1b84qg4/migrate_11_to_12_on_new_hardware/

- Disable all jobs, perform necessary backups and snapshots of existing v11 server
- Perform upgrade to v12
- Post upgrade, take configuration backup
- On new v12 server, perform configuration restore
- Enable jobs
- Decom old VBR server/DB.

Or you can install the same v11 version on the new server, perform the config backup and restore first, then do an in place upgrade of the new server to v12.

Make sure you upgrade any VeeamONE and Enterprise Manager first.

Licensing, you can use the same license on both servers as long as its part of the migration process...only running the same license on two different VBR server in production at the same time is an issue.

Veeam Duplicate UUID

This is to bypass the UUID check if you have restored an old back to new hardware for example a laptop or physical PC.

REGEDIT

To ‘EnableSystemUuidFailover’ key should be added on each Veeam Agent host with non-unique ID.

This is the key enabling Veeam failover logic.

Name: EnableSystemUuidFailover
Path: HKLM\SOFTWARE\Veeam\
Type: DWORD
Value: 1

Then a unique ID should be assigned manually on each Agent station.
Another Veeam registry should be added on each host for it:

Name: SystemUuid
Path: HKLM\SOFTWARE\Veeam\
Type: REG_SZ
Value: {a custom UUID}

Custom UUID should correspond with the standard UUID format rules, brackets are required.

You can use some online generator for it (https://www.uuidgenerator.net/) or put some your own strings there.

Rescan protection group and you are deployed now

Disable "Windows recovery image file not found" warning

You can add AgentsDisableRECollectionWarning key here HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication to disable this warning.
Name: AgentsDisableRECollectionWarning
Path: HKLM\SOFTWARE\Veeam\
Type: DWORD
Value: 1

WordPress - Setup WordPress

Connecting to Your Server

Using PuTTY

Open PuTTY and enter your domain name in the box named **Host name (or IP address)** and enter the port number used to connect to SSH under **Port**, and then click **Open**. You can even save your site settings by entering a name in the **Saved Sessions** box and by pressing **Save**. Next time, you can always load the session by selecting your site and clicking **Load**.

PuTTY will now ask for your username. Enter your username and press **Enter**. Now you will be asked for your password. Note here that while you are typing your password, you won't see it being typed on the screen. It's hidden for security reasons. Press **Enter** after you've typed your password, and you will be logged on.

Using Any Other SSH Client or Mac Terminal

Enter the following command in your Terminal client to connect to your site's command-line over SSH:

```
ssh username@domain.com -p 22
```

The `-p` switch tells it to use port number 22. If your host allows SSH over default port 22, you can omit `-p` and `22` in the above command; otherwise, substitute 22 for your host's SSH port number. After logging in, you will see something like this:

```
domain.com@username:-$
```

That's the shell command prompt where you will be typing all your commands from now on.

2. Downloading WordPress

Now that we have logged in to our SSH server, we need to go to the correct directory where we want to set up our blog. Then we download the files and extract them there. Let's say the directory you want your blog to be installed under is **blogdemo** residing under the **public_html** directory. In that case, you will use the following command:

```
cd public_html/blogdemo/
```

Now that we have reached the correct directory, we will download WordPress using the `wget` command.

```
wget http://wordpress.org/latest.tar.gz
```

```
$tar xfz latest.tar.gz
```

The above command downloads the latest WordPress install from their server and extracts the file from it into the **blogdemo** directory. `x`, `f`, and `z` are parameters which tell the tar command to extract the contents from the specified file using gzip.

Now, after extraction, you will find a **wordpress** directory under the **blogdemo** directory containing your install. So to shift the files back to where they should be, use the following commands:

```
mv wordpress/* ./
```

This command moves the contents of the **wordpress** directory into the current directory. Anytime you want to check what's in the current directory, type `ls`.

If you want, you can use the following commands to delete both the **wordpress** directory and the archive file you downloaded:

```
rmdir ./wordpress/
```

```
rm -f latest.tar.gz
```

File Permissions

Correct file permissions from the root folder

When you setup WP you (the webserver) may need write access to the files. So the access rights may need to be loose.

```
chown www-data:www-data  -R * # Let Apache be owner
find . -type d -exec chmod 755 {} \;  # Change directory permissions rwxr-xr-x
find . -type f -exec chmod 644 {} \;  # Change file permissions rw-r--r--
```

After the setup you *should* tighten the access rights, according to Hardening WordPress all files except for wp-content should be writable by your user account only. wp-content must be writable by *www-data* too.

```
chown <username>:<username>  -R * # Let your useraccount be owner
chown www-data:www-data wp-content # Let apache be owner of wp-content
```

Maybe you want to change the contents in wp-content later on. In this case you could

- temporarily change to the user to *www-data* with `su`,
- give wp-content group write access 775 and join the group *www-data* or
- give your user the access rights to the folder using ACLs.

Whatever you do, make sure the files have rw permissions for *www-data*.

3. Installing WordPress

In this step, we will create the database and corresponding user and associate them together. Then we will use the famous five-minute install of WordPress to finish it off.

Note: Before moving ahead, you will need to check whether you have got the privileges to create a database or not. An easy way to check is to go to your phpMyAdmin and check whether you can create a database from there or not. If you can't, that means you won't be able to follow this step. You should check with your web host if they allow you to do so or not. Most shared web hosts will let you create a database.

First, you need to log in to the MySQL command-line using the following command:

```
mysql -u username -p
```

After entering this, you will be asked for your MySQL password. Type your password and you will be shown a screen like this:

Now that we have logged in to the MySQL Server, we will first create a database and will grant the user access to that database. Use the following commands now:

```
create database dbname;
```

```
grant usage on *.* to username@localhost identified by 'password';
```

```
grant all privileges on dbname.* to username@localhost;
```

Don't forget the semi-colon at the end of each MySQL command. The first command creates the database. The second command allows the user to connect to the database. The final command grants all privileges to the user for that database. You can test whether your database creation was successful by running this command:

```
use dbname;
```

It should say "database changed". Now you can exit the MySQL command-line by typing `exit`.

Now fire up the blog in your browser and run the usual WordPress install, and use the database information we used in the third step to set up your **wp-config.php** and then set up your blog.

Note: New Database User

In our tutorial, we are using an existing database user to connect to the new database. But if you want a separate user for each database, you need to create a new user to access that database. Here's how you should do it.

Once you are inside the MySQL shell, use the following commands to create a new user and set its password.

```
create user 'dbusername'@'localhost' identified by 'password';
```

Now go back to Step 3 and run all other commands with this username.

Editing wp-config.php

In our tutorial, I have told you that after doing everything on the shell, you can directly proceed to the install. But some of you might want to edit **wp-config.php** to add special settings and code. You can only do that via the shell. While you are in your blog directory at the shell, use the following command to fire up the Vim Editor (a command-line shell file editor)

```
vi ./wp-config.php
```

Now you will see something like what's shown below:

Vim Editor
Image not found or type unknown

Press the `i` key to enter insert mode, and use the arrow keys to move around the file. Once you have made your edits, press the **Esc** key to exit insert mode. To exit Vim, type `:` and then type `wq` and press **Enter**. This will save your changes and quit Vim.

Increasing Import File Size

Create a .user.ini in the root folder of the WordPress site

```
upload_max_filesize = 500M
post_max_size = 500M
memory_limit = 500M
max_execution_time = 600
```

Or you can change the following in the wp-content/plugins/all-in-one-wp-migration/constants.php

```
define( 'AI1WM_MAX_FILE_SIZE', 2 << 28 );
```

To the following

```
define( 'AI1WM_MAX_FILE_SIZE', 2 << 500 );
```

All in one Import for restore after the file is on the root/wp-content folder and does not require a paid version.
Original

all-in-one-wp-migration-6.7.zip

Forked direct link

All-In-One-WP-Migration-With-Import-master.zip

Download and Install WordPress With the WP-CLI Tool

In this section, I'll show you an even better way to download and install WordPress: with the WP-CLI tool. First, we have to install the WP-CLI tool on the server.

How to Install the WP-CLI Tool

Run the following commands on your server to download, install, and configure the WP-CLI tool.

```
curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

```
chmod +x wp-cli.phar
```

```
sudo mv wp-cli.phar /usr/local/bin/wp-cli
```

Let's check if the WP-CLI tool is installed successfully by using the following command.

```
wp-cli --info
```

You should see something like this:

```
OS:     Linux 4.15.0-91-generic #92-Ubuntu SMP Fri Feb 28 11:09:48 UTC 2020 x86_64
```

```
Shell:
/bin/bash
```

```
PHP binary:
/usr/bin/php7.2
```

```
PHP version:
7.2.24-0ubuntu0.18.04.3
```

```
php.ini used:
/etc/php/7.2/cli/php.ini
```

```
WP-CLI root dir:
phar://wp-cli.phar/vendor/wp-cli/wp-cli
```

```
WP-CLI vendor dir:
phar://wp-cli.phar/vendor
```

```
WP_CLI phar path:
/etc/init.d
```

```
WP-CLI packages dir:
```

```
WP-CLI global config:
```

```
WP-CLI project config:
```

```
WP-CLI version:
2.4.0
```

Download and Install WordPress

Let's download the latest version of WordPress first.

```
wp-cli core download
```

If the download is successful, you'll see something like the following:

```
Downloading WordPress 5.5.1 (en_US)...
```

```
md5 hash verified: 72c6f56b4818ffd0e6e6a4ed8f3e8d4e
```

```
Success: WordPress downloaded.
```

So we've downloaded the WordPress codebase now.

Next, it's time to create the **wp-config.php** file. We can do it with the help of the following command. Replace the placeholders with the actual values. I assume that you've already created the database which you would like to use with WordPress.

```
$wp-cli config create --dbname=YOUR_DB_NAME --dbuser=YOUR_DB_USERNAME --dbpass=YOUR_DB_PASSWORD
```

```
Success: Generated 'wp-config.php' file.
```

Finally, let's run the following command, which installs WordPress.

```
$wp-cli core install --url=YOUR_DOMAIN_NAME --title=YOUR_BLOG_TITLE --admin_user=ADMIN_USERNAME --admi
```

```
Success: WordPress installed successfully.
```

And with that, WordPress is installed successfully on your server!

In fact, the WP-CLI tool is capable of doing a lot more than just installation. It allows you to manage plugins and themes and do any necessary version updates as well.

VMWare - Install Windows 11 on vCenter 8 without TMP 2.0

Create a VMWare to host Windows 11 without having a virtual TMP or device installed.

Once you are at this step you have to hit "Shift-F10" to open up the command prompt

image.png
Image not found or type unknown

Once the command prompt window is opened type "regedit"

image.png
Image not found or type unknown

Once opened then navigate to "HKEY_LOCAL_MACHINE, SYSTEM, Setup" and then right-click and add a "New, Key"

image.png
Image not found or type unknown

Add the key called "LabConfig" then right-click on the "LabConfig" and add a new "DWORD Value"

image.png
Image not found or type unknown

Add the new value called "ByPassTPMCheck" with a hexdecimal of "1"

image.png
Image not found or type unknown

Close every window then click on "Install Now" but do not reboot or the new added key will be lost.

image.png
Image not found or type unknown

File Transfer - Using FTP

LFTP commands

FTP

Commands

to resume a single file upload using the built-in ftp command you will need to know how many bytes of the file you have already sent. This should be accessible by using `ls`. Then you use the following sequence to restart your upload replacing `<#>` with the number of bytes already sent and `<filename>` with the filename you are uploading.

```
restart <#>
put <filename>
```

If the server allows it you should receive a message such as the following...

```
350 Restart position accepted (<#>).
150 Ok to send data.
```

This will resume your upload.

LFTP

Using the LFTP command this allows you to restart a died ftp session

Commands

The following command is the login to the server and go to the folder you are placing the file in

```
lftp user:pass@host/path/to/folder
```

```
lftp user:pass@host/path/to/folder
cd ok, cwd=/path/to/folder
lftp user@host:/path/to/folder> reput file.ext
---> TYPE I
<--- 200 Type set to I
---> SIZE file.ext
<--- 213 11842837120
---> PASV
<--- 227 Entering Passive Mode (10,211,14,15,220,70).
---- Connecting data socket to (10.211.14.15) port 56390
---- Data connection established
---> ALLO 20769244058
<--- 202 No storage allocation necessary
---> REST 11842837120
<--- 350 Restarting at 11842837120. Send STORE or RETRIEVE to initiate transfer
---> STOR file.ext
<--- 150 Opening BINARY mode data connection for file.ext
`file.ext' at 6756302848 (32%) 31.50M/s eta:7m [Sending data]
```

This command is to restart the failed FTP replace the "file.txt" with your file

```
reput file.txt
```

After a quick search, there's a command line program called `lfvi sftp` that provides ftp mirroring functionality.

Adapted from a guide here, something like this should do the trick:

```
#!/bin/bash
HOST='address.co.uk'
USER='myuser'
PASS='mypass'
TARGETFOLDER='/public_html/java/desktop/'
SOURCEFOLDER='deploy/'

lftp -f "
open $HOST
user $USER $PASS
lcd $SOURCEFOLDER
mirror --reverse --delete --verbose $SOURCEFOLDER $TARGETFOLDER
bye
"
```

I'd suggest you'd do it without the `--delete` until you're sure you've got the arguments right!

File Transfer - WPUT

WPUT

This is to resume a files transfer using wput instead ftp or lftp commands and can be used in Windows or Linux

WPUT Commands

Here is an example how wput continues upload after connection problems:

```
wput -v -u -B upload.zip ftp://login:pass@server.com/dir/upload.zip
--20:14:23-- `upload.zip'
    => ftp://login:xxxxx@111.111.111.111:21/dir/upload.zip
Connecting to 111.111.111.111:21... connected!
Logging in as login ... Logged in!
==> CWD dir
==> TYPE I ... done.
==> SIZE upload.zip ... done (4313 bytes)
==> PASV ... done.
==> REST 3584 ... done.
==> STOR upload.zip ... done.
Length: 902,153,406 [902,149,822 to go]
 7% [======>                                                                ] 65,658,368       194.0K/s ETA
1:10hError: Error encountered during uploading data (Operation now in progress)
==> ABOR ... Error: recv() timed out. No data received
Receive-Warning: read() timed out. Read '' so far.
failed.
Waiting 10 seconds... Error: recv() timed out. No data received
Receive-Warning: read() timed out. Read '' so far.
Connecting to 111.111.111.111:21... connected!
Logging in as login ... Logged in!
==> CWD dir
==> TYPE I ... done.
==> SIZE upload.zip ... done (65247144 bytes)
```

```
==> PASV ... done.
==> REST 65246208 ... done.
==> STOR upload.zip ... done.
Length: 902,153,406 [836,907,198 to go]
 9% [++++++==>
```

File Transfer - CURL

CURL

This is the resume a file transfer using curl instead ftp or lftp commands and can be used in Windows or Linux

CURL Commands

```
curl -C - --upload-file source_file ftp://destination.server.com/
```

Asus - OpenVPN Site to Site or Point to Point

ASUS Asuswrt Merlin

Most of the documents online are missing steps or the folks writing the document are assuming that the folks setting this up are network traffic wizards.

GOAL:

With one of the Asus routers being the server and the other being a client, we want to be able from either side hit IPs or hostnames of any of any device.

Both Routers:

VPN Type: TUN as TAP maybe overkill for this case

Protocol: UDP

Static Routes: Both servers

When you export the OpenVPN certificates from the router (as opposed to supplying your own), they have the CN set as '**client**'. This is relevant/confusing for the server config, as our other router is a client named client.

Server:

ASUS RT-AC5300 with 192.168.53.1/24

Interface Type	◉TUN ○TAP
Protocol	○TCP ◉UDP
Server Port	1196 (Default : 1194)
Authentication Mode	◉TLS ○Static Key
Keys and Certificates	Edit...
Username/Password Authentication	○Yes ◉No

TLS control channel security *(tls-auth / tls-crypt)*	Encrypt channel
HMAC Authentication	
VPN Subnet / Netmask	10.100.100.0 255.255.255.0
Advertise DNS to clients	◉ Yes ○ No
Data ciphers	AES-128-GCM:AES-256-GCM:AES-128-CBC:AES-256-CBC
Compression	LZO Adaptiv
Log verbosity	3 (Between 0 and 6. Default: 3)
Manage Client-Specific Options	◉ Yes ○ No
Allow Client <-> Client	◉ Yes ○ No
Allow only specified clients	○ Yes ◉ No

Allowed Clients

Common Name(CN)	Subnet	Mask	Push	Add / Delete
			No	

client	192.168.51.0	255.255.255.0	Yes	

Custom Configuration

```
reneg-sec 432000
push "route 192.168.53.0 255.255.255.0"
route 192.168.51.0 255.255.255.0
```

Custom Explained:

```
reneg-sec 432000 #optional
push "route 192.168.53.0 255.255.255.0" #server LAN IP
route 192.168.51.0 255.255.255.0 #client LAN IP
```

Export the .ovpn files from the new server config

Client:

ASUS RT-AC5300 with 192.168.51.1/24

Import .ovpn config file exported from server, to set the certificates and some of the basic settings.

Select client instance	▼
Service state	Image not found or type unknown
Automatic start at boot time	○Yes ○No
Description	Site-to-Site HOUSE
Import .ovpn file	Choose a file Upload

Network Settings	
Interface Type	○TUN ○TAP
Protocol	○TCP ◉UDP
Server Address and Port	Address:XXXXXXX.asuscomm.com Port: 1196
Create NAT on tunnel	○Yes ◉No Routes must be configured manually.
Inbound Firewall	○Block ◉Allow
Accept DNS Configuration	Disabled ▼
Redirect Internet traffic through tunnel	▼

Authentication Settings	
Authentication Mode	◉TLS ○Static Key
Username/Password Authentication	○Yes ◉No

Crypto Settings	
Keys and Certificates	Edit...
Data ciphers	AES-128-GCM:AES-256-GCM:AES-128-CBC:AES-256-CBC

Crypto Settings	
TLS control channel security ***(tls-auth / tls-crypt)***	Encrypt Channel ▼
Auth digest	▼

Advanced Settings	
Log verbosity	3 (Between 0 and 6. Default: 3)
Compression	LZO Adaptiv ▼
TLS Renegotiation Time	-1 (in seconds, -1 for default)
Connection Retry attempts	0 (0 for infinite)
Verify Server Certificate Name	No ▼

Custom Configuration

```
resolv-retry infinite
float
keepalive 15 60
remote-cert-tls server
```

Applied the "automatic start at boot time"

Turn on the client VPN

Server Connection:

OpenVPN Server 2 - Running

Clients

Common Name Username	Real Address Virtual Address	MBytes Received	MBytes Sent	Connected Since
client	XXX.XXX.XXX.XXX:47361 10.100.100.2	7305.28	2561.14	2024-12-22 09:49:57

Routes

Virtual Address	Common Name	Real Address	Last Ref
192.168.51.217C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:29
192.168.51.1C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:31
192.168.51.15C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:36
10.100.100.2	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:50
192.168.51.109C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:28
192.168.51.145C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:50
192.168.51.10C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:31
192.168.51.101C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:25
192.168.51.140C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:40
192.168.51.9C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:50
192.168.51.23C	client	XXX.XXX.XXX.XXX:47361	2024-12-22 11:03:44

Confusion:

The problem is that from the server I cannot access the the LAN on the client side without adding a route vis the JFFS scripts folder using the "nat-start" script.

```
#!/bin/sh
#https://github.com/RMerl/asuswrt-merlin.ng/wiki/User-scripts
#
DATE=$(date +"%Y-%m-%d-%H%M%S")
echo "deleting the route to router if it exists" $DATE >> /tmp/nat-start.log
route delete -net 192.168.51.0 netmask 255.255.255.0 gw 10.100.100.2
echo "done deleting the route" $DATE >> /tmp/nat-start.log
echo "adding route to router" $DATE >> /tmp/nat-start.log
route add -net 192.168.51.0 netmask 255.255.255.0 gw 10.100.100.2
echo "done adding route to router" $DATE >> /tmp/nat-start.log
```

References:

https://medium.com/@kylemattimore/asuswrt-merlin-openvpn-tunnel-site-to-site-69b9011b079a

https://www.senia.org/2018/03/12/router-to-router-vpn-tunnel-using-asus-routers/

https://www.asus.com/us/support/faq/1011706/

MarkDown - Guide .md

Markdown Cheat Sheet

Thanks for visiting [SFL Services LLC](https://www.sflservicesllc.com)!

This Markdown cheat sheet provides a quick overview of all the Markdown syntax elements. It can’t cover every edge case, so if you need more information about any of these elements, refer to the reference guides for [basic syntax](https://www.markdownguide.org/basic-syntax/) and [extended syntax](https://www.markdownguide.org/extended-syntax/).

Basic Syntax

These are the elements outlined in John Gruber’s original design document. All Markdown applications support these elements.

Heading

H1
H2
H3

Bold

bold text

Italic

italicized text

Blockquote

> blockquote

Ordered List

1. First item
2. Second item
3. Third item

Unordered List

- First item

- Second item
- Third item

Code

`code`

Horizontal Rule

Link

[Markdown Guide](https://www.markdownguide.org)

Image

Extended Syntax

These elements extend the basic syntax by adding additional features. Not all Markdown applications support these elements.

Table

Syntax	Description
Header	Title
Paragraph	Text

Fenced Code Block

```
{
  "firstName": "John",
  "lastName": "Smith",
  "age": 25
}
```

Footnote

Here's a sentence with a footnote. [^1]

[^1]: This is the footnote.

Heading ID

My Great Heading {#custom-id}

Definition List

term
: definition

Strikethrough

~~The world is flat.~~

Task List

- [x] Write the press release
- [ ] Update the website
- [ ] Contact the media

Emoji

That is so funny! :joy:

(See also [Copying and Pasting Emoji](https://www.markdownguide.org/extended-syntax/#copying-and-pasting-emoji))

Highlight

I need to highlight these ==very important words==.

Subscript

H~2~O

Superscript

X^2^

Certificate - PKCS12

https://stackoverflow.com/questions/68832952/need-a-little-help-to-generate-p12-cert

https://stackoverflow.com/questions/10175812/how-to-generate-a-self-signed-ssl-certificate-using-openssl?rq=1

DELL - XPS Killer Wifi

I was only getting 1.5mb transfer and 60mb web download

WARNING -- Changing the registry can break your machine if done wrong!!! Do so at your own risk!

I had (sounds like) the same WiFi issues you are having. I was able to "fix" it with a registry hack. Go to this key Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings**19cbb8fa-5279-450e-9fac-8a3d5fedd0c1** and create a value (if not there) Attributes with a DWORD value of 2.

Go a little further down, under the above key to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\19cbb8fa-5279-450e-9fac-8a3d5fedd0c1\12bbebe6-58d6-4636-95bb-3217ef867c1a**DefaultPowerSchemeValues\381b4222-f694-41f0-9685-ff5bb260df2e** and add the same Attributes value here or set it to 2 if it's already there. Under this key, change the DCSettingIndex to 0 (zero) to match the ACSettingIndex.

This makes the WiFi card use full power on battery under the Balanced Power Plan which is the default plan.

Also mentioned in my previous posts was to remove all the Killer software and use the Intel drivers instead. The current version works fine. Of course download the Intel drivers before removing the Killer stuff. This did not fix the issue by itself but trust the Intel drivers more.

Caffeine Hack - Got caught with Caffeine installed

Hack

Click Start, then type `Powershell` and it should show up.

Type `notepad $profile` to open your default profile.

This will likely be blank if this is the first time doing this.

Paste the following code:

```
function idle {
$wshell = New-Object -ComObject wscript.shell;
"Press CTRL+C to cancel."
while ($true) {
$wshell.SendKeys('+')
Sleep 60
}
}
```

Close PowerShell, then re-open it (see step one).

Type `idle` and hit enter.

Optional: autorun you can add idle to line 9, and when opening PowerShell it will auto run

This function just presses the shift key every minute. It's less intrusive than mouse wigglers..

Updated Version

Save this to your profile, and then you can run it indefinitely using `idle` or set a duration in minutes by adding it at the end `idle 28800`.

You can even have it do the math for you. So 60 mins * 8 hours would be `idle (60*8)`.

You can get even fancier if you know what time you need to clock out.

```
# If you stop working at 5pm (17:00) then you could use this:
$peaceout = (get-date 17:00)

idle ($peaceout - (get-date)).TotalMinutes
```

This part goes in your profile. Remember, if you make changes to your profile you will need to close and reopen any PowerShell terminals for them to pick up the changes.

```
function idle {
    param(
    [int]$Duration = -1 # Duration in Minutes
    )
    $wshell = New-Object -ComObject wscript.shell;

    'Press CTRL+C to cancel.'
    $idle = $true

    while ($idle) {
    $wshell.SendKeys('+')
    if ($Duration -eq 0) {
    $idle = $false
    'Time Expired.'
    break
    }
    elseif ($Duration -gt 0) {
    write-host -NoNewline "`r$Duration min(s) remaining."
    $Duration--
    }

    Start-Sleep 60
    }
}
```

> For both you have to save the file under my documents in the following folder and name the file the following:

> \Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1

Script Hack

```
param(
    [switch]$Indefinite,
    [int]$Minutes = 0
)

if ($Indefinite) {
    Write-Host "Keeping system awake indefinitely. Press Ctrl+C to stop."
    while ($true) {
        [System.Windows.Forms.Cursor]::Position
        Start-Sleep -Seconds 60
    }
} elseif ($Minutes -gt 0) {
    Write-Host "Keeping system awake for $Minutes minutes. This window will close automatically when done."
    $endTime = (Get-Date).AddMinutes($Minutes)
    while ((Get-Date) -lt $endTime) {
        [System.Windows.Forms.Cursor]::Position
        Start-Sleep -Seconds 60
    }
    Write-Host "Time's up!"
} else {
    Write-Host "Please specify either -Indefinite or -Minutes <number of minutes>."
}
```

To Use the Script:

To keep the system awake indefinitely, run:

```
.\keep-awake.ps1 -Indefinite
```

To keep the system awake for a specific number of minutes (e.g., 30 minutes), run:

```
.\keep-awake.ps1 -Minutes 30
```

Synology - Host Unifi for FREE on Synology NAS

All you have to do is ass a scheduled task scripts under tasks and run the following

```
docker run -d --name=Unifi-Controller \
-p 3478:3478/udp \
-p 10001:10001/udp \
-p 5514:5514/udp \
-p 8080:8080 \
-p 8443:8443 \
-p 8880:8880 \
-p 8843:8843 \
-e PUID=1026 \
-e PGID=100 \
-e TZ=Europe/London \
-v /volume1/docker/unifi:/config \
--restart always \
ghcr.io/linuxserver/unifi-controller
```

Concrete - Dry Pour Schedule

image.png
Image not found or type unknown

Synology - Upgrade 1515+ to 1517+

Worked like a charm

image.png
Image not found or type unknown

https://github.com/prt1999/Synology_model_upgrade

Ran the above process

image.png
Image not found or type unknown

Forum Discussions

https://xpenology.com/forum/topic/69328-converting-ds1515-into-ds1517-dsm-72/page/3/

https://xpenology.com/forum/topic/69328-converting-ds1515-into-ds1517-dsm-72/

Revert Back to 1515+

Synology DOM module pinout

Plug into the 2nd row, i.e. straight pins, with normal USB assignment.
2 red
4 white
6 green
8 black

PiHole - Configuration

This is a great link for pi-installation

https://www.crosstalksolutions.com/the-worlds-greatest-pi-hole-and-unbound-tutorial-2023/

ESXi - UPS Nut Installation

Vmware ESXi NUT Client Installation and Configuration

Requirements

- You must have a NUT server connected to a UPS and configured in your environment.
- SSH must be enabled on your ESXi installation
- Community acceptance level must be enabled on your ESXi installation in order to install the client

Download

Download the latest **NutClient-ESXi-x.x.x-x.x.x-offline_bundle.zip** package from:

https://github.com/rgc2000/NutClient-ESXi/releases.

Install

- Secure copy the **NutClient-ESXi-x.x.x-x.x.x-offline_bundle.zip** to your ESXi server's /tmp directory by either using WinSCP/pscp in Windows or scp in Linux.
- Set ESXi Community Acceptance level:

```
esxcli software acceptance set --level=CommunitySupported
```

If you get the following error:

```
[AcceptanceConfigError]
Secure Boot enabled: Cannot change acceptance level to community.
Please refer to the log file for more details.
```

You must disable Secure Boot in your computer BIOS and re-try the installation again.

- Install bundle:

```
esxcli software vib install -d /tmp/NutClient-ESXi-x.x.x-x.x.x-offline_bundle.zip
```

- If installation was successful you should see the following output:

```
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Margar_bootbank_upsmon_x.x.x-x.x.x
   VIBs Removed:
   VIBs Skipped:
```

- You can now delete the files in the /tmp directory and disable the SSH service if desired.

ESXi Configuration

- In the ESXi Web client, navigate to **Host —> Manage —> System —> Advanced Settings**. In the **Search** box enter **UserVars**.**Nut (Figure 1).**

Figure 1

image-1647104283497.png
Image not found or type unknown

- Configure the following variables:

NutUpsName: Name of the UPS on the NUT server (in the form of inverter_name@server_name or server_ip). Several inverters can be entered separated by a space. There will be no system shutdown until the last UPS still standing has given the shutdown command.

NutUser: Name of the NUT server login account

NutPassword: NUT Server Connection Account Password

NutFinalDelay: Seconds to wait after receiving the low battery event to shut down the system

NutSendMail: Set to 1 for the NUT client to send an e-mail to each important event of the UPS

NutMailTo: E-mail address to send UPS events to

- In the ESXi Web client, navigate to **Host —> Manage —> Services —> NutClient —> Actions —> Policy —> Start and Stop with Host (Figure 2).**

Figure 2

image-1647104294686.png
Image not found or type unknown

- In the ESXi Web client, navigate to **Host —> Manage —> Services —> NutClient —> Actions —> Start (Figure 3).**

Figure 3

image-1647104306878.png
Image not found or type unknown

Tips

- Use the ESXi host configuration tab in the vSphere Client to decide how to start and stop (or suspend) virtual machines. This order will be respected by the UPS shutdown procedure.
- The clean shutdown of the OS in the virtual machines is only possible if the vmware tools are installed.
- To uninstall the NUT client, use the following command:

```
esxcli software vib remove -n upsmon
```

- To update the NUT client, use the following command:

```
esxcli software vib update -d /tmp/NutClient-ESXi-x.x.x-x.x.x-offline_bundle.zip
```

- To estimate the time needed for the server to shut down on UPS alert, type the command below on the host ESXi (by ssh or on the console). The shutdown procedure is immediately started:

```
/opt/nut/sbin/upsmon -c fsd
```

- If the NUT Client is configured correctly, the ESXi /var/log/syslog.log should have a message similar to below where ups@UPSHOST is the ups name and the UPS host you setup earlier :

```
2019-09-22T13:28:07Z upsmon[2111424]: Communications with UPS ups@UPSHOST established
```

Synology - Flash uboot ROM

This guide describes a method how to restore u-boot if the flash has been completely erased. This situation can arise if there was a power loss during u-boot upgrade or you accidentally deleted the boatloader while playing with the u-boot commands like I did. There are many reasons why the DiskStation fails to boot, but as long as the u-boot bootloader partition is not destroyed, you can repair the flash image using the u-boot serial flash subsystem. This guide is for all who are sure that u-boot has been corrupted and that there is no other way to recover.

The solution is to physically replace the corrupted flash chip and restore its original content. I will be using a Dangerous Prototypes Buspirate for serial console access and to flash the firmware externally onto a brand new flash IC. This of course will void your warranty as you have to replace the old chip with the new one. In case you are not experienced with soldering you will risk destroying the mainboard, but in my opinion this is still better than throwing the bricked unit away. The following steps involve the preparation of the flash.rom image, programming and replacing the old chip. The new installation will be verified with the serial console.

1. Download and extract firmware image

This guide is for a DS213j, but should work equally on other NAS.

https://global.download.synology.com/download/DSM/release/6.2/23739/DSM_DS213j_23739.pat

The pat file is an uncompressed tar archive: $ tar -xvf DSM_DS213j_4458.pat The files we need are:
- uboot_DS213jv10.bin: u-boot
- zImage: kernel
- rd.bin: initrd

2. Prepare the flash.rom image

The size of the flash chip on the DS213j is 64Mbit, so we need an 8MB large image. We first recall the flash layout to get the right offsets:
00000000:000bffff RedBoot (uboot) 000c0000:0038ffff zImage 00390000:007cffff rd.gz 007d0000:007dffff vender 007e0000:007effff RedBoot_Config 007f0000:007fffff FIS_directory

Create an empty flash image of 8 MB size filled with zeros: $ dd if=/dev/zero of=flash.rom bs=1024 count=8192 Copy the uboot image to the beginning of the file not truncating the rest: $ dd if=uboot_DS213jv10.bin of=flash.rom conv=notrunc Now copy the kernel image at the right offset. dd cannot directly use hexadecimal values. These have to be converted by the shell: $ dd if=zImage of=flash.rom bs=1 seek=$((0xc0000)) conv=notrunc Next is the initrd image: $ dd if=rd.bin of=flash.rom bs=1 seek=$((0x390000)) conv=notrunc Then comes the vender partition. This is not provided in the download of the firmaware as this is unique to your DiskStation and written only once in the factory. It contains the serial number and the MAC address, which can be

found on the sticker at the back of the case. The DiskStation will boot without the vender information, but without the MAC address it will assign a random MAC at each boot. This will annoy DHCP servers as they serve a new IP on every reboot. Automatic firmware updates and the DS Assistant rely on the MAC address as well.

For the next step you will need the serial number and original MAC from the sticker and a hex editor (I use hexeditor). First we create an empty 64 kB vender partition: $ dd if=/dev/zero of=vender.img bs=1024 count=64 The MAC address is stored in the first 6 bytes and the 7th byte contains a checksum. The checksum is calculated by taking the sum of the bytes in the MAC address. The following C program can be used to calculate the checksum. The checksum is stored in an unsigned char, which is not large enough to store the total. It will flow over give the rest, which is larger than multiples of 256 bytes:
#include <stdio.h> int main() { unsigned char chksum = 0; int i = 0; unsigned char rgAddr[6] = {0x00, 0x11, 0x32, 0xFF, 0xFF, 0xFF}; for (i = 0; i < 6; i++) { chksum += rgAddr[i]; } printf("Checksum: 0x%X\n", chksum); return 0; } The first three bytes are the Synology part, the last three bytes needs to be changed to your MAC address. Compile with $ gcc -o checksum mac_checksum.c This MAC example 00:11:32:FF:FF:FF will give a checksum of 0x40.

Insert these bytes into the image: $ hexeditor -b vender.img 00000000 00 11 32 FF FF FF 40 The serial number is written like this. For example:
SN=1350LAN009999,CHK=999
00000020 53 4e 3d 31 33 35 30 4c 41 4e 30 30 31 39 39 39 00000030 2c 43 48 4b 3d 39 39 39
Use an ascii to hex converter to generate the hex values. The checksum is calculated on next reboot automatically and can be inserted later. We use a dummy of 999 for now. Once u-boot is working again, you can flash the updated vender image from u-boot (see below how to do this). Now insert the vender data into the flash image: $ dd if=vender.img of=flash.rom bs=1 seek=$((0x7d0000)) The flash.rom image is now ready to be flashed onto the chip. The RedBoot_Config and FIS_directory partitions are not needed.

3. Flash the rom image to the new chip

The flash chip on the DS213j is a Micron 25Q064A 13E40 64Mbit serial flash. I bought mine here
https://hbe-shop.de/Art-2253680-MICRON-N25Q064A13ESE40E-FLASH-SERIELL-64MB-3V-8WSOIC

What you also need is a SOIC/DIL 8POL adapter PCB to connect the IC to a breadboard:
https://hbe-shop.de/Art-1136592-ARIES-08-350000-11-RC-ADAPTER-SOIC-DIL-8POL

For the SPI programmer and 3.3V TTL-USB Level shifter I use a Dangerous Prototypes Buspirate:
http://dangerousprototypes.com/docs/Bus_Pirate

The Buspirate is a multi purpose debugging and prototyping device that has SPI, JTAG, UART and

I2C modes. Solder the IC onto the SOIC adapter and then you can use breadboard to connect the Buspirate with the following circuit (http://flashrom.org/Bus_Pirate):

Image not found or type unknown

For the actual programming of the flash.rom image I used flashrom (http://flashrom.org/Flashrom), which supports the Buspirate programmer directly: $ sudo flashrom -c "N25Q064..3E" -V -p buspirate_spi:dev=/dev/ttyUSB0,pullups=on -w flash.rom Now we are set to replace the flash chip on the main board.

4. Replace the flash chip on main board

This is the most difficult part and if you are inexperienced with a soldering iron you should get some practise by de-soldering IC's from old motherboards or scrap electronics. Did I mention that touching the DiskStation PCB with a soldering iron will void your warranty? To de-solder the flash chip the trick is to apply plenty of solder over all pins. The pins will be connected through a thick layer of solder and this will distribute the heat over the pins and keep the solder liquid long enough. This looks messy at first, but it is then possible to apply heat to both sides of the chip simultaneously and lift the IC from the PCB without damaging the pins. If you were successful in de-soldering the flash, you could even spare yourself the hassle of buying a new chip and flashing the old one. I use de-soldering wick to clean the pins of the IC and the pads on the PCB. Then I remove residue flux from the PCB with residue cleaner or isopropanol using an old toothbrush. With the same technique you have to de-solder the IC from the SOIC adapter. Before soldering the reprogrammed chip back in, make sure the pads are free from old solder and shiny clean. Then fix the chip on the board with tape and apply very little solder to two opposite pins first, and afterwards apply solder to the remaining pins.

5. Connecting a serial console

Information on how to connect to the serial console can be found here:

http://www.fr.netbsd.org/ports/sandpoint/instSynology.html

The serial console of the DS213j is available at the 6 pin jumper next to the 3 pin fan connector. Connect the BusPirate pins GND, MISO and MOSI to the jumper pins 2, 4 and 6.

Image not found or type unknown

Pin Function BusPirate
1 3.3 V
2 GND GND
4 TX MISO (RX)

6 RX MOSI (TX)

Start your favourite terminal program and put the BusPirate into UART transparent bridge mode. $ script -f -c "picocom -b 115200 /dev/ttyUSB0" session.log Now it is time to power on the DiskStation and watch the output on the console. If the re-flashing was successful, you should see u-boot loading kernel and initrd images. If you still have DSM installed on the hard drives, the DiskStation should boot normally now, otherwise it will stop at the initrd prompt. You could use the DS Assistant to do a fresh DSM install. Congratulations, you are almost there!

6. Flashing the vendor image using u-boot

The DiskStation will complain that the serial number checksum does not match the one provided (999) and prints the correct checksum on the console. Write it down and update the vender.img with the correct serial number using hexeditor.

EDIT: The checksum of the 13 digit serial number equals to the sum of the individual character bytes, for example SN=1350LAN009999,CHK=744

Now reboot and interrupt the boot process with CTRL-C to get to the u-boot prompt. Copy the vender.img to a TFTP server and set the Diskstation IP with ipaddr and the TFTP server address with serverip. Then transfer the image to memory address 0x2000000: Marvell>> setenv ipaddr 192.168.1.50 Marvell>> setenv serverip 192.168.1.10 Marvell>> tftpboot 0x2000000 vender.img Now initialise the flash subsystem, erase mtd3 partition and write the 64 kB vender.img to the correct address 0x7d0000: Marvell>> sf probe 0 Marvell>> sf erase 0x7d0000 10000 Marvell>> sf write 0x2000000 0x7d0000 0x10000 Marvell>> reset The DiskStation is now restored to a fully working condition. If further problems arise, it is always a good idea to connect the serial console first to see if u-boot is still working. From here you can manually flash new kernel and initrd images or fix problems with the network.

Have a good day!
Alexander

https://community.synology.com/enu/forum/17/post/69287

HPE - iLO4 Reflash after Not Responsive 380p Gen8

iLO 4 firmware in Direct Mode

Download Online ROM Flash Component for Linux - HPE Integrated Lights-Out 4 (CP######.scexe)

https://support.hpe.com/connect/s/product?language=en_US&ismnp=0&l5oid=5219994&cep=on&kmpmoid=5219994&tab=driversAndSoftware&driversAndSoftwareFilter=8000029

Attached is 2.82 version of iLO4 CP053894.scexe

Download Service Pack for ProLiant 2016+ (search on torrents) version 8.1 or use this ISO

Using HP USB Key Utility for Windows, we create a bootable flash drive from the SPP image.

For Windows use RUFUS https://rufus.ie/en/ to create a usb boot from the SPP .iso file

For Linux installation use https://unetbootin.github.io/ to create a usb boot

Copy CP053894.scexe to the finished flash drive in /hp/swpackages

Turn off the power, remove the case. On the system board, find the main dip switch (System maintenance switch) and turn the first (S1) switch to the ON position

Load the server from the SPP flash drive

Once on the image screen you need to select Interactive mode and when the main menu loads very slowly

press ctrl + alt + d + b + x to launch the console

Run:

You need to enter a simple magic command:

rmmod hpilo

then Run:

sh /mnt/bootdevice/hp/swpackages/CP027578.scexe --direct

After successful iLO flashing, turn off the power and return the first (S1) switch back (OFF).

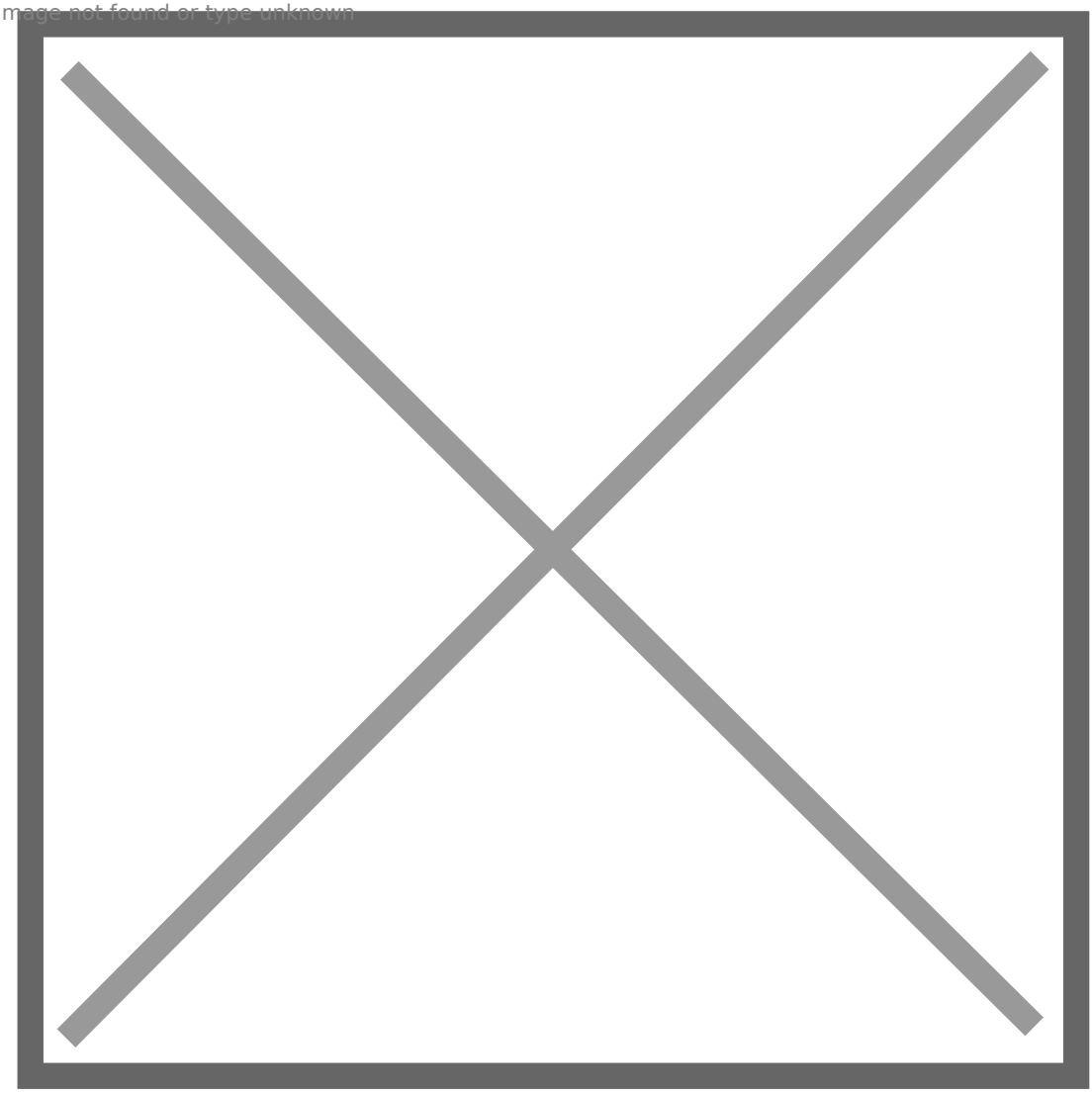
image.png
Image not found or type unknown

VMWare - Copy and Paste from Console to VM

On any Powered Off VM, click the "**Advanced Parameters**" tab.

1. Click filter icon of Attribute column. Search for 3 items' names, check if they already exist. If yes, edit their corresponding values. If not, add them from the textboxs above.

Image not found or type unknown



Name	Value
`isolation.tools.copy.disable`	`FALSE`
`isolation.tools.paste.disable`	`FALSE`

isolation.tools.setGUIOptions.enable	TRUE

2. Click "**OK**".

3. Power on the VM
4. Then use Copy/Paste directly on Windows/Linux/any other platform.

MailServer - Test SMTP

Your best, easiest and most globally available tool: **telnet or Windows CMD**

1. At command prompt, type: telnet mail.mailserver.com 25
2. Type EHLO , and then press ENTER.
3. Type AUTH LOGIN. The server responds with an encrypted prompt for your user name.
   Enter your user name encrypted in base 64. You can use one of several tools that are available to encode your user name.
   The server responds with an encrypted base 64 prompt for your password. Enter your password encrypted in base 64.
4. Type MAIL FROM:, and then press ENTER. If the sender is not permitted to send mail, the SMTP server returns an error.
5. Type RCPT TO:,and then press ENTER.If the recipient is not a valid recipient or the server does not accept mail for this domain, the SMTP server returns an error.
6. Type DATA.
   If desired, type message text, press ENTER, type a period (.), and then press ENTER again.
   If mail is working properly, you should see a response similar to the following indicating that mail is queued for delivery:
   250 2.6.0 MAILID-SOMETHINGHERE@mail.somedomain.com.

ImageMagick - Install on Redhat 9 from Source

Installing ImageMagick 7 from Source Code

To install ImageMagick from source, you need a proper development environment with a compiler and related development tools. If you don’t have the required packages on your system, install development tools as shown:

```
sudo yum groupinstall 'Development Tools'
sudo yum -y install bzip2-devel freetype-devel libjpeg-devel libpng-devel libtiff-devel giflib-devel zlib-devel ghostscript-devel djvulibre-devel libwmf-devel jasper-devel libtool-ltdl-devel libX11-devel libXext-devel libXt-devel lcms-devel libxml2-devel librsvg2-devel OpenEXR-devel php-devel
```

Now, download the latest version of the ImageMagick source code using the following wget command and extract it.

```
sudo wget https://www.imagemagick.org/download/ImageMagick.tar.gz
sudo tar xvzf ImageMagick.tar.gz
```

Configure and compile the ImageMagick source code. Depending on your server hardware specs, this may take some time to finish.

```
sudo cd ImageMagick*
sudo ./configure
sudo make
sudo make install
```

Verify that the ImageMagick compile and install were successful.

```
sudo magick -version
```

```
Version: ImageMagick 7.0.8-28 Q16 x86_64 2019-02-19 https://imagemagick.org
Copyright: © 1999-2019 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP
Delegates (built-in): bzlib djvu fontconfig freetype jng jpeg lzma openexr pangoca
```

IPCamera - Different Configs

CAMERA LIST

MODEL	CONNECTION
ASH43-W	rtsp://admin:□□□□□□□□@192.168.50.101:554/cam/realmonitor?nel=1&subtype=0
DAHAUA	HTTP:85
IP5M-T1179EW-AI-V3	HTTP:80

HPE - ProLiant DL380p Gen8 GPU Install

Supported GPUs for the HP ProLiant DL380p Gen8 are limited by the server's specific PCIe risers, 225W power constraints, and passive cooling requirements. Official and community-tested options include the **NVIDIA GRID K1, K2**, **Tesla P100**, **Quadro K6000**, or consumer cards like the **NVIDIA Tesla M4/M60**

Because the DL380 G8 requires specific hardware components for proper installation, you will need to pay attention to the following details:

- **Hardware & Riser Kits:** You will need the HP Double Wide Riser Cage Kit (`662885-B21`) and the Secondary GPU Riser (`728543-B21`) to accommodate double-wide or full-height GPUs.
- **Power Cables:** Standard server power cables will not fit most NVIDIA GPUs. You will need a custom 10-pin to 8-pin GPU power cable to draw power from the motherboard.
- **Power Supply:** Operating dual GPUs requires dual 1200W power supply units (PSUs) and two physical processors installed
- **BIOS Configuration:** For advanced GPUs (like the Tesla P100), you must enter the BIOS, press **Ctrl + A** at the main screen to reveal the "Service Options," and enable **PCI Express 64-bit BAR Support**.
- **iLO & POST Issues:** Many modern GPUs (like RTX series) can trigger POST code 5808, halting the boot process. Ensure your server has the latest BIOS update and iLO firmware to minimize compatibility issues.
- **Card Compatibility:** The server officially supports specific enterprise cards like the NVIDIA Quadro K4000/K5000/P2000 and Grid K1/K2. Consumer cards (like the GTX 1050, GTX 1650, or RTX series) often require BIOS modifications, external power adapters, and custom chassis modification

Dell - Hard Drive Capacity Difference Between Drives

The capacity difference between the two drives is caused by **differing logical block/sector formatting** or **OEM vendor provisioning (HPA / Max LBA limits)**.

Even within the same Western Digital / Ultrastar DC HC520 12TB family, SAS drives are deployed with different low-level format structures:

1. Different Sector Formats (512e vs. 4Kn vs. Enterprise 520/528 Bytes)

- **Standard 12TB:** Typically reports around **11,175.5 GB** (11.17 TiB) when formatted with standard 512-byte emulation (`512e`) or 4096-byte native (`4Kn`) sectors.
- **Enterprise SAN/EMC Formats:** Drives pulled from proprietary SAN enclosures (EMC, NetApp, Huawei) often use **520-byte or 528-byte sectors** (or Type 1/2 Data Integrity Field protection). When translated or truncated by a Dell PERC/HBA, the usable LBA count drops, showing up around **10,948.5 GB**.

2. OEM Firmware & Provisioning (HPA / Max LBA)

If one drive came from an OEM vendor (e.g., NetApp, EMC, Cisco, HPE) and the other is a generic Dell/retail drive, the OEM firmware may restrict the drive's total accessible Logical Block Addressing (LBA) count via Host Protected Area (HPA) or factory provisioning.

How to Fix / Match Them

To get disk `0:1:3` to match `0:1:4` at full capacity:

1. **Check the Sector Size:**
   Boot into a Linux live environment (or pass the drive through via HBA/IT-mode) and run:
   Bash

```
smartctl -i /dev/sdX
# or
sg_scan -i
```

Check the `Logical block size` and `Formatted with type 1/2/3 protection` values.

2. **Low-Level Format to Standard 512e / 4Kn:**
   Using the `sg3_utils` package in Linux, reformat the drive to standard 512-byte or 4096-byte sectors:
   Bash

   ```
   # Reformat to standard 512-byte sectors:
   sg_format --format --size=512 /dev/sdX
   ```

   (Note: This is a low-level format that will erase all data on that specific disk and takes several hours for a 12TB drive.)
3. **Reset Max LBA (if sector size is already 512):**
   If the drive was already 512 bytes, reset any HPA/LBA clamp:
   Bash

   ```
   hdparm -N /dev/sdX
   # To restore full native capacity:
   hdparm -N p[max_lba_value] /dev/sdX
   ```

Once reformatted, the Dell PERC controller will detect `0:1:3` at the full **11175.5 GB** size.