|  |
| --- |
| **JDN Standards – Dell VRTX** |

Introduction 2

User & password guidelines 2

Standard configuration 3

VRTX Identification 4

VRTX Indicators (buttons, LEDs and LCD) 5

VRTX User replaceable parts 7

VRTX Rack conversion 7

Suggested rack layout 8

Dell VRTX firmware 10

Dell VRTX remote management configuration 11

On-board VRTX storage configuration 15

Installation preparation 17

VMWare Essentials Plus 5.5 installation 18

Dell storage performance tweaks 20

VMWare vCenter appliance 20

Template/OVA deployment 23

DC deployment 24

VM deployment 24

ISO deployment 25

Manual deployment of additional VMs 25

Synology NAS configuration 26

UPS configuration 26

Veeam backup configuration 26

Other useful documentation 26

# Introduction

This document describes the technical setup of the standards as defined for JDN deployments in 2014. This document is specific to JDN ships & remote sites and should not be seen as relevant for THVs or headoffices.

This document focuses on the Dell VRTX solution used for the large & medium-sized deployments (as described in the [deployment guidelines](http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed82ce5e79)) and only takes a brief look at the network, NAS & UPS configuration.

# User & password guidelines

The “**root**”, “**administrator**” & “**admin**” user accounts & passwords are reserved for installation and SA/SE usage. Which of the three user names is used can depend on the system in question. They should never be communicated to the crew (even the Captain).

A separate “**adl\_tse**” user (with the same user rights) will be created for TSE usage. This will enable TSE to always use the same login on all devices. Ideally, TSE should never use the “root”, “administrator” & “admin” passwords after the installation has been concluded and the normal support cycle has started.

A separate “**adl\_local**” user will be created to be communicated to the Captain (and potentially ELEC). Depending on the device in question, only restricted rights will be granted to the adl\_local user.

Passwords chosen will be different for each ship or site, and as such should be diligently registered in RDM for each ship or site.

# Standard configuration

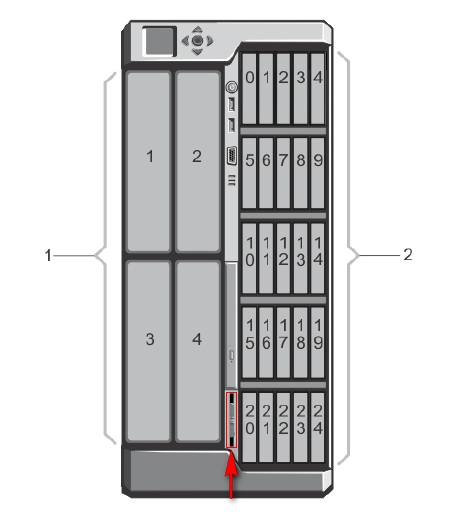
The standard configuration consists of:

* Server:
  + Dell VRTX
    - 2 to 3 M630 (previously M520) blades with each:
      * two Xeon CPUs
      * 96GB RAM
      * Two 600GB SAS 2.5” disks
    - Passthrough networking module
    - Redundant (S)PERC
    - Redundant CMC
    - 4 1100W PSUs
    - 16 600GB SAS 2.5” disks for normal Medium & Large setups and 25 600GB SAS 2.5” disks for Large Offshore
* Networking:
  + Firewall:
    - Single SRX240 or Redundant SRX240
  + Switches:
    - Redundant Juniper EX3300 (48 & 24 port)
    - Redundant Juniper EX2200 (48 port, only for small offices)
    - SFP+ DAC twinax cables
  + Serial device server:
    - Moxa NPort 5610-16 (for offshore vessels only, TBD)
* Backup storage:
  + Redundant Synology RS815+ (previously RS814+) (4x4TB or 4x8TB for offshore)   
    or Synology DS1515+ (5x4TB)
* UPS:
  + Optional APC Smart-UPS SRT 6000VA, 3000VA or 2000VA
* Time server:
  + Meinberg LANTIME M300 GLN-SQ/LNE with GPS/Glonass antenna
* Software:
  + VMWare Essentials Plus 5.5
  + ESET Endpoint Security
  + Veeam 8

Consult the deployment guidelines for more information:

<http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed824d5fa5>

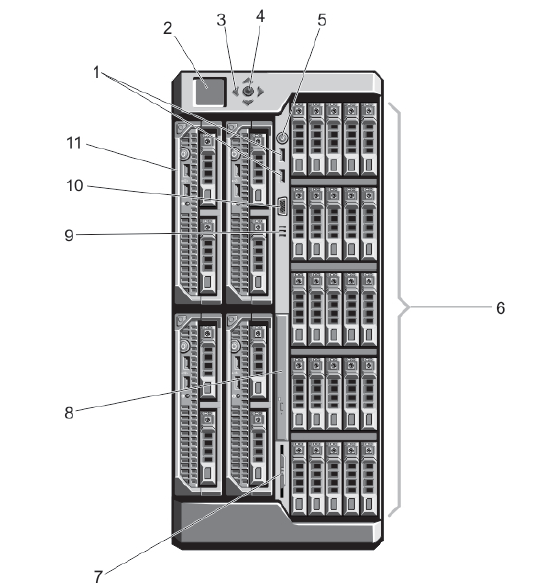
# VRTX Identification



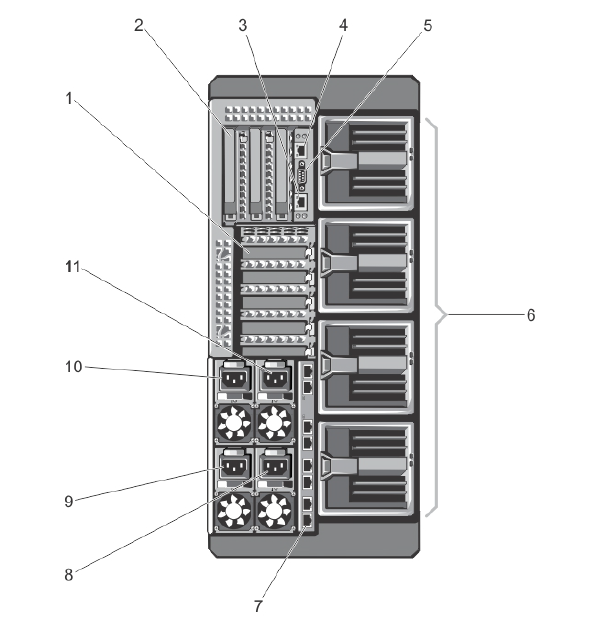
1. On the left: Blade numbers
2. On the right: 2.5” disk numbers

* Marked in red: information tag with JDN ID tag & Dell service tag location (pull out)

# VRTX Indicators (buttons, LEDs and LCD)



1. USB connectors
2. LCD panel
3. LCD menu scroll buttons
4. Select/Enter
5. Power button
6. Hard drives
7. Information tag (Dell service tag & JDN tag)
8. Optical drive (not present)
9. Vents
10. Video connector
11. Server modules



1. Low profile PCIe expansion card slots
2. Full height PCIe expansion card slots
3. CMC NIC port 2
4. CMC NIC port 1
5. Serial connector
6. Blower modules
7. I/O module ports (passthrough in our standard)
8. Power supply PSU4
9. Power supply PSU3
10. Power supply PSU1
11. Power supply PSU2

(PSU 1 & 2 and PSU 3 & 4 are paired if power grid redundancy mode is activated)

# VRTX User replaceable parts

Dell VRTX:

* fans,
* fan assembly,
* blower,
* blower assembly,
* LCD display,
* control panel,
* PERC 8 RAID controllers,
* CMC,
* PSU,
* disks

Dell M520 (& M620/M630) blade:

* RAM,
* CPU,
* disks

# ~~VRTX Rack conversion~~

**OBSOLETE**

~~Required tools:~~

* ~~Screwdrivers:~~
  + ~~Philips #1 & #2~~
  + ~~Torx T6 (key provided, but easier with screwdriver), T8, T10, T15 (long screwdriver advisable) & T20~~

~~Required parts:~~

* ~~Dell VRTX Tower configuration~~
* ~~Dell VRTX tower-to-rack conversion kit~~
* ~~Dell VRTX rack mounting kit (rack rails)~~

~~Dell documentation for conversion steps:~~ [~~http://www.dell.com/support/Manuals/us/en/19/Topic/PERVRTXOM-v1/en-us/GUID-CD2C81E8-2BA5-4C83-8D41-B7A41A24AB3E~~](http://www.dell.com/support/Manuals/us/en/19/Topic/PERVRTXOM-v1/en-us/GUID-CD2C81E8-2BA5-4C83-8D41-B7A41A24AB3E)

~~Be aware that conversion takes 30 to 45 minutes as it requires detailed disassembly of the system.~~

~~Using a modified procedure, the conversion takes 15-20 minutes. Consult~~ [~~http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed8243348d~~](http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed8243348d) ~~for the optimized conversion procedure.~~

~~Conversions deal with lots of small parts and require quite a bit of room to work in.~~

~~Be sure to ground yourself before handling sensitive electronics.~~

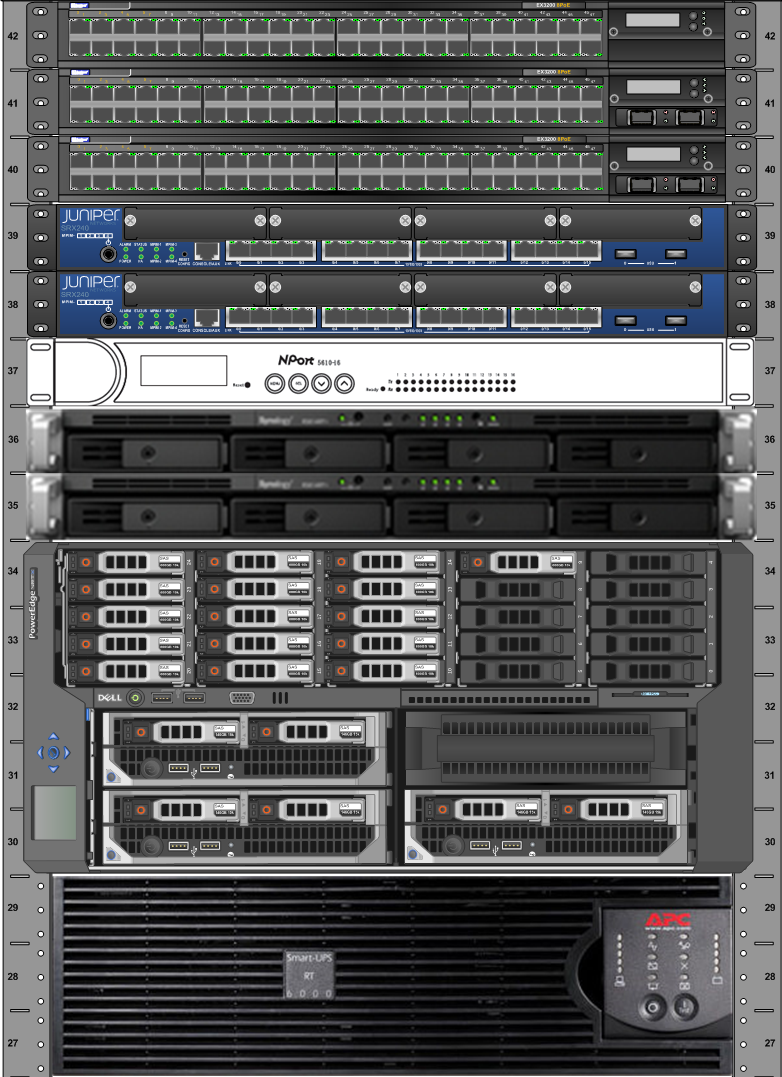
# Suggested rack layout

If a rack is present, the suggested rack layout is as follows (top to bottom):

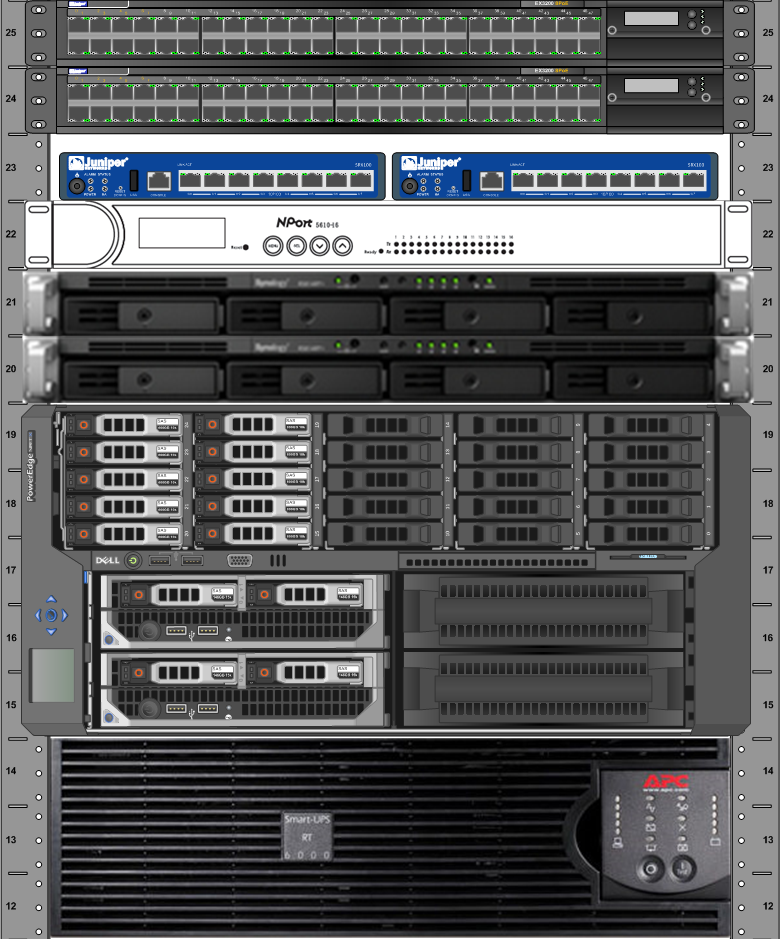
* Firewalls
* Switches
* Serial server (if applicable: offshore vessels only)
* NAS
* Dell VRTX
* UPS

It is suggested to start mounting these from top to bottom (applying upwards pressure when securing the equipment into the rack). In previous tests, the firewalls, switches & serial server were found to be sticking out too far, preventing the following rail kit from being mounted properly. In this case, it is advised to skip a row of mounting points to ensure the following equipment is mounted flush to each other.

Large setup:



Medium setup:



The items above are mounted using the manufacturer’s suggested rack mounting procedures as supplied with the kits, with the exception of the Synology NAS. The Synology rack mount kit rails do not lock the NAS in place when slid into the rack. Due to a ship’s movement, this could cause the NAS to move. To prevent this, we advise to use a long rack mounting screw (not supplied in the rail kit) through the NAS’s front bracket to secure it in place. This should be done on only one side of the unit, as it will be sufficient to lock it firmly in place. The other side of the unit can use the standard Synology recommended mounting method.



*Synology recommended mounting procedure, using the supplied screws.*



*JDN ship mount procedure for Synology, using a long rack mounting screw.*

# Dell VRTX and blade firmware

The VRTX’s planar board (motherboard) requires a recent firmware to be able to use redundant SPERC8 raid controllers. Without the newer firmware, the VRTX will only be able to use a single non-redundant SPERC8 controller.

The CMC firmware must be version 2.04 or higher to be able to provide advance logging and troubleshooting while using Write-Back write caching when two PERC8 controllers are installed on the planar.

Make sure the firmware of the VRTX (CMC, SPERC8, planar) and blades (iDRAC, motherboard, PERC) are up to date! This firmware can be found under :   
[\\jdn-file01\Ict\_New\_Standard\_Sites\_Vessels\Firmware\Current](file:///\\jdn-file01\Ict_New_Standard_Sites_Vessels\Firmware\Current)

The CMC must be updated with separate packages. The blades can also be updated with loose packages through the IDRAC but also a bootable ISO is available. This file is in the folder itself of the type of blade on the network share. For example :   
[\\jdn-file01\Ict\_New\_Standard\_Sites\_Vessels\Firmware\Current\Dell M630 blades\LinuxIso](file:///\\jdn-file01\Ict_New_Standard_Sites_Vessels\Firmware\Current\Dell%20M630%20blades\LinuxIso)  
You can mount the ISO through the virtual console in the iDRAC and update all firmwares this way, or create an USB stick from this ISO and attach it to the front of each blade.  
Do this firmware update for each blade.

# Dell VRTX remote management configuration

Turn on the Chassis and Blades.

**CMC (Dell VRTX):**

* Connect both CMC network ports to the network.
* Configure CMC IP using the built-in *Control Panel LCD* (x.x.x.250)
* Do not register IP in DNS
* Do not configure iDRACs yet, since it’s a lot easier to do it from the web interface
* Rotate LCD display to rack mode if applicable
* Log into the CMC by browsing to its IP and entering “root” “calvin” as credentials. You will be prompted to modify the default password. Be sure to save this password in a safe location (RDM?).
* In the side menu, select “Chassis Overview”.
  + In the top menu, select “Troubleshooting”.
    - Under the “Diagnostics” tab: Enter the command “*racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 128*” and press “Submit”. This will allow NTP to work properly. Without this setting, NTP might not work as intended due to the distance between the ships & the NTP servers in case the local NTP server cannot be reached.
  + In the top menu, select “Setup”.
    - Under the “General tab”:
      * Enter the ship’s or site’s shortened name, followed by a -VRTX01 in the “Chassis Name” field. Increment 01 if there is already a VRTX on board. Example: VGR-VRTX01 for the Voyager test ship.
      * Enter the ship's or site's name in the “Chassis Location” field.
      * Press “Apply”.
    - Under the Date/Time tab: Enable NTP, add NTP servers “172.16.3.22”, “10.128.1.72” & “NTP1.oma.be” and select UTC as the time zone before pressing “Apply”.
  + In the top menu, select “Network”.
    - Under the “Network” tab:
      * At the IPv4 section, enter “x.x.x.11” as the Static Preferred DNS Server where x.x.x is the ship’s Admin\_Trust range and “8.8.8.8” as the Static Alternate DNS Server.
    - Under the “Services” tab:
      * Scroll to the “SNMP Configuration” heading:
        + Check “Enabled”.
        + Enter “Community Name”: SNMP-RO
      * Scroll to the “Remote Syslog Configuration” heading:
        + Check “Enabled”.
        + Enter “Syslog Server 1” as x.x.x.25 where x.x.x is the admin\_trust IP range.
  + In the top menu, select “Power”.
    - Under the (power) “Configuration” tab: For the Redundancy Policy setting, select “Grid Redundancy”. (PSU 1 & 2 will be fully redundant for PSU 3 & 4 and vice versa, keep this in mind when connecting power leads!)
  + In the top menu, select “User Authentication”.
    - Under the “Local Users” tab, select the first free user (should be “2”).
    - Select “enable user”.
    - Enter “User Name” “adl\_tse”.
    - Enter a newly generated password in the “Password” & “Confirm Password” fields. Be sure to save this password in a safe location (RDM?).
    - From the “CMC Group” drop down, select “Administrator”. All checkboxes below should automatically be checked.
    - Click “Apply”.
    - Under the “Local Users” tab, select the first free user (should be “3”).
    - Select “enable user”.
    - Enter “User Name” “adl\_local”.
    - Enter a newly generated password in the “Password” & “Confirm Password” fields. Be sure to save this password in a safe location (RDM?).
    - From the “CMC Group” drop down, select “Power User”. Some checkboxes below should automatically be checked.
    - Click “Apply”.
  + In the top menu, select “Alerts”.
    - Under the “Email Alert Settings” tab:
      * For deployments **without** a commbox enter:
        + SMTP server: smtp.jandenul.com
        + Source email address: srv\_backup\_xxx@jandenul.com where xxx is the site ID   
          (example: [srv\_backup\_ede@jandenul.com](mailto:srv_backup_ede@jandenul.com))
        + Note: this user/address will need to be created and the IP needs to be whitelisted by SA.
      * For deployments **with** a commbox enter:
        + SMTP server: <admin\_trust-range>.17
        + Source email address: <hostname>@<prefix>.jandenul.com (example: PRO-VRTX01@pro.jandenul.com)
      * Under “Email Alert Destinations”, under first entry, enter:
        + Destination email address: [ICT-ServiceDesk@jandenul.com](mailto:ICT-ServiceDesk@jandenul.com)
        + Name: JDN Service Desk
      * Press “Apply”.
    - Under the “Chassis Events” tab:
      * Make sure “Enabled” is checked (Apply if needed).
      * For “System Health”, “Storage” & “Audit”, select all “Critical” and “Warning” events, and select all Email, SNMP & Remote Sys Log.
      * Press “Apply”.
  + In the top menu, select “Setup”.
    - Under the “Chassis Backup” tab: Click “Save” to Save Chassis Configuration. Keep this file in case you have to restore it while installing the setup.
* In the side menu of the CMC’s web interface, select “Front Panel”.
  + In the top menu, select “Setup” > “Configuration”.
  + Select the check box next to “Lock Control Panel LCD”.
  + Press “Apply” at the bottom of the page.

**iDRAC (Dell M520/M630 blades):**

* When logged into the CMC, in the side menu, select “Chassis Overview” > “Server Overview” > “Slot-01”.
* In the top menu, select “Setup”.
* Enable the iDRAC's IPv4 LAN, manually configuring the correct IP address (x.x.x.251 for Blade 1, x.x.x.252 for Blade 2, x.x.x.253 for Blade 3).
* Return to the properties.
* Click “Launch iDRAC GUI” & log in. Default credentials are “root” “calvin”.
* You will be prompted for a new password.
* On the side menu, click “Overview” > “Server” and in the top menu “Properties” > “Details”.
* Scroll down to the end of the page and enter the ship's or site's name in the datacenter field. Press “Apply”.
* On the side menu, click “iDRAC settings” and in the top menu “Properties” > “Settings”.
* Check the box next to “Enable Network Time Protocol (NTP)” and enter the IP of the local domain controller as “NTP Server 1”. Usually this will be “172.16.3.22” for ships with a time server on board. For sites, the domain controller’s IP can be used.
* On the side menu, click “Overview” > “Server” > “Alerts”.
  + Under the “SNMP and Email settings” tab:
    - Fill out 10.x.x.25 as the “Destination Address” and check the box under “State” in the “IP Destination List” section. Fill out the “Community String” as SNMP-RO.
    - Enable SNMP v2 in the “SNMP Trap Format” section.
    - Fill out [ICT-ServiceDesk@jandenul.com](mailto:ICT-ServiceDesk@jandenul.com) in the “Destination Email Addresses” section.
    - Under the “SMTP (Email) Server Address Settings” section fill out:
      * For deployments **without** a commbox enter:
        + SMTP server: smtp.jandenul.com
        + Source email address: [srv\_backup\_xxx@jandenul.com](mailto:srv_backup_xxx@jandenul.com), where xxx is the Site ID (example: [srv\_backup\_ede@jandenul.com](mailto:srv_backup_ede@jandenul.com))
        + Note: this user/address will need to be created and the IP needs to be whitelisted by SA. The iDRAC can use authentication.
      * For deployments **with** a commbox enter:
        + SMTP server: <admin\_trust-range>.17
        + Source email address: <hostname>@<prefix>.jandenul.com (example: [PRO-iDRAC01@pro.jandenul.com](mailto:PRO-iDRAC01@pro.jandenul.com))
    - Click “Apply”.
  + Under the “Alerts” Tab:
    - Make sure “Enabled” is checked (Apply if needed).
    - For “System Health”, “Storage” & “Audit”, select all “Critical” and “Warning” events, and enable email alerts.
    - Press “Apply”.
* On the side menu, click “Overview” > “iDRAC Settings” > “Network”.
  + Under the “Services” tab:
    - Scroll to SNMP “Agent”.
    - Check “Enabled”.
    - Enter “SNMP Community Name”: SNMP-RO
    - Check SNMP Protocol : All
    - Press “Apply”.
* On the side menu, click “iDRAC settings” > “User Authentication”.
  + Under the “Local Users” tab, select the first free user.
  + In the “User Main Menu” screen, select “Configure User” and press “Next”.
  + Select “enable user”.
  + Enter “User Name” “adl\_tse”.
  + Enter a newly generated password in the “Password” & “Confirm Password” fields. Be sure to save this password in a safe location (RDM?).
  + Under “IPMI User Privileges” for the “Maximum LAN User Privilege Granted” drop down, select “Administrator”
  + Under “iDRAC User Privileges”, select “Administrator” for the “Roles” drop down. This should select all checkboxes below.
  + Click “Apply”.
  + Under the “Local Users” tab, select the first free user.
  + In the “User Main Menu” screen, select “Configure User” and press “Next”.
  + Select “enable user”.
  + Enter “User Name” “adl\_local”.
  + Enter a newly generated password in the “Password” & “Confirm Password” fields. Be sure to save this password in a safe location (RDM?).
  + Under “IPMI User Privileges” for the “Maximum LAN User Privilege Granted” drop down, select “Operator”
  + Under “iDRAC User Privileges”, select “Operator” for the “Roles” drop down. This should select all checkboxes below.
  + Click “Apply”.
* Repeat all steps under this section for all blades that are present in the VRTX.

*Note: The CMC NICs have no VLANs configured. The switches should tag them as Admin\_Trust.*

# On-board VRTX storage configuration

The standard storage configuration of the disks keeps 2 disks as global host spares & puts the remainder of the disks in Raid 6.

Virtual disks are created with the size of 1,5 TB maximum (ESX best practice). Naming conventions are VirtualDisk*X*R*6*, where the *X* is an incrementing number and *6* is the used raid level.

All these virtual disks are made available to all ESXi servers.

Step by step procedure:

* Log into the CMC.
* Shut down all blades.
* Browse to the "Storage > Controllers > Troubleshooting" section.
* For each SPERC make sure they are “active”. If not, select the "Enable RAID controller" option for the disabled raid controller and press “Apply”. This will reboot your storage component. This will take a while.
* Execute the following Virtual Disk creation steps if you use the **16 disk setup**:
  + In the side menu, select “Storage” > “Virtual Disks”.
  + At the top of the “Virtual Disks” screen, select “Create”.
  + First scroll down and select the physical Internal Disks you wish to use. Standard configuration leaves the first two disks unselected (for later use as hot spare). Select all remaining disks.
  + Scroll back up and enter the name of your virtual disk. Typically this is VirtualDisk1R6, where 1 is the sequence number and R6 is the raid type.
  + Select raid level. Typically Raid 6.
  + Set capacity to 1,5 TB.
  + Scroll to the bottom of the page & click “Create Virtual Disk”.
  + Repeat the Virtual Disk creation steps until all capacity has been used for virtual disks. Don't forget to select the appropriate raid level, or the correct disks will not be displayed. The last disk will not have a full 1,5 TB, but this is not a problem. If the final disk is below 500GB, add it to the previous disk, making the final disk a maximum size of ±2 TB.  
    If you use the standard 16 disk setup, you will have the following virtual disks:
    - VirtualDisk1R6: 1.50 TB (used for the vCenter, DC & templates)
    - VirtualDisk2R6: 1.50 TB (used for servers)
    - VirtualDisk3R6: 1.50 TB (used for clients)
    - VirtualDisk4R6: 2.04 TB (used for the file server)
* Execute the following Virtual Disk creation steps if you use the **25 disk setup**:
  + In the side menu, select “Storage” > “Virtual Disks”.
  + At the top of the “Virtual Disks” screen, select “Create”.
  + First scroll down and select the physical Internal Disks you wish to use. This configuration leaves the first disk unselected (for later use as hot spare). Then select the first 12 disks following the first for the first array and the remaining 12 (except the first) for the second array.
  + Scroll back up and enter the name of your virtual disk. This is Ar1VirtualDisk1 (for Array 1 Virtual Disk 1), where 1 is the sequence number for the array & the virtual disk.
  + Select raid level. Typically Raid 6.
  + Set capacity to 2 TB.
  + Scroll to the bottom of the page & click “Create Virtual Disk”.
  + Repeat the Virtual Disk creation steps until all capacity has been used for virtual disks using the following sizes & names:
    - Ar1VirtualDisk1: 2TB (used for the vCenter, DC & templates)
    - Ar1VirtualDisk2: 2TB (used for servers)
    - Ar1VirtualDisk3: 1.55 TB (spare)
    - Ar2VirtualDisk1: 2TB (used for clients)
    - Ar2VirtualDisk2: 2TB (used for the file server)
    - Ar2VirtualDisk3: 1.55 TB (spare)
* Allowing multiple assignment of Virtual Disks to blades:
  + In side menu, select “Storage”.
  + In the top menu, select “Setup”.
  + Scroll down, select “Multiple Assignment” and press “Apply”
* Configure hot spares:
  + In side menu, select “Storage” > “Physical Disks”.
  + In the top menu, select “Setup”.
  + Use the drop down to set Physical disks 0:0:0 & 0:0:1 as “Global Hot Spare” if you use the 16 disk setup, and only Physical disks 0:0:0 if you use the 25 disk setup.
* Go to "Storage > Virtual Disks > Manage" and make sure write policy “Write Back” is enabled. If not select "Edit Policy: Write Cache" and pick "Write Back" instead of “Write Through” for all your virtual disks. The change above will be carried out immediately, but it is still suggested to reset the CMC once more under "Chassis Overview > Power > Control" with "Reset CMC (warm boot)".
* Boot your previously shut down blades.

# Installation preparation

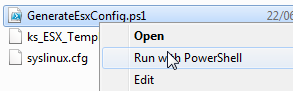
Installation has been largely automated to speed up deployments. The scripts are written under the assumption that they will be executed on a clean environment.

The installation steps below require some preparation:

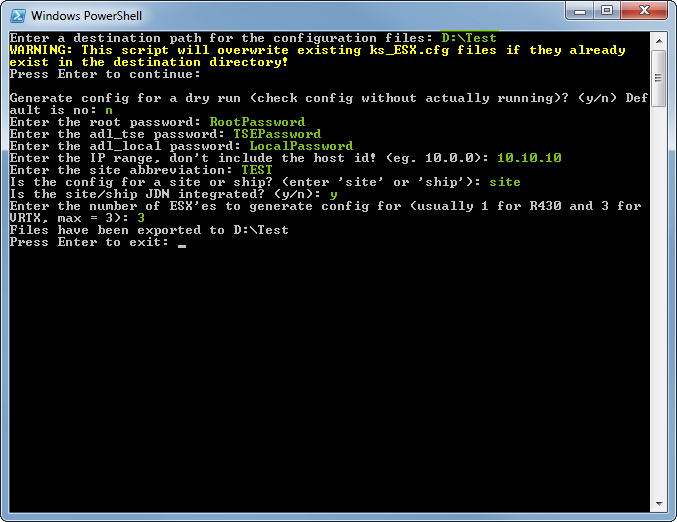
* The necessary files can be found at [\\jdn-file01\Ict\_New\_Standard\_Sites\_Vessels](file:///\\jdn-file01\Ict_New_Standard_Sites_Vessels) and should be copied locally to F:\Standaarden\... for easy access (assuming F:\ is your external disk or your data partition). The “deprecated” folders can be ignored, however if you are going “on site” for your installation it can be wise to include them as well in case of issues with the current files. **The folder structure should be maintained as is, since the provided scripts have references to files and folders relative to their position.**
* To be able to execute the provided scripts, a few programs should be installed on your computer. Ideally these will be included as default software for TSE, but in the meanwhile install these manually:
  + VMware ovftool 4.0 or higher.
  + Powershell 3.0 or higher.
  + PowerCLI 6.0 or higher.
* During the installation of PowerCLI, you will be prompted to allow execution of scripts by setting Set-ExecutionPolicy. Make sure Powershell Execution Policy is set correctly, as none of the scripts will work without this.
* If the scripts pop up strange errors, first troubleshoot by executing:  
  *Add-PSSnapIn VMware.VimAutomation.Core*
* Since a bootable USB stick must be created, you will need a program to do this. The default JDN software for this is Rufus and this should already be installed on all TSE laptops. Unetbootin is included as well to have an alternative.

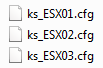
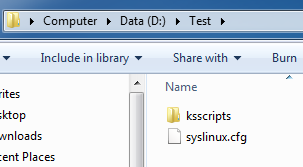
Modify your locally copied scripts:

* Under ...\Scripted Install\ESXi install stick\Dell VRTX\ksscripts\ edit the .cfg files in accordance with the comments present within the file. You will need to configure one config file for each blade.
  + Or, use the script from the 'Generate\_ESX\_Config' folder.



Just follow the steps in the script and fill in the requested values according to your setup (see items in green in the screenshot)



The necessary config files will be generated.

* Under ...\Scripted Install\Scripts\ edit the Configuration.xml file in accordance with the comments present within the file. Do not edit the .txt or StartThisElevated files.

Bootable USB stick preparation:

* Use Rufus or Unetbootin to create a bootable USB stick from the dell customized ESXi ISO file. These should be located under ...\Software\Current\Virtualization\
* Copy the files from ...\Scripted Install\ESXi install stick\Dell VRTX\ or the ones generated by the script into the root directory of your newly created USB stick.

# VMWare Essentials Plus 5.5 installation

In this section we install VMWare ESXi 5.5 on the blades’ local storage (2 SAS disks in Raid 1), using an ESX Dell customized image which contains the (S)PERC drivers required to see the shared VRTX storage. (If you use the standard non-custom installer, you will need to add the megaraid\_sas drivers manually or you will not be able to see the shared storage.)

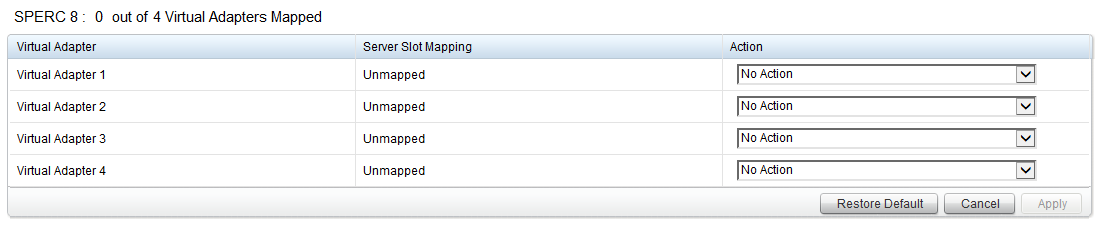
The USB stick used to install ESXi can contain a large part of the required configuration in a so-called “kickstart” script. These kickstart scripts will need to be modified to fit your specific environment.

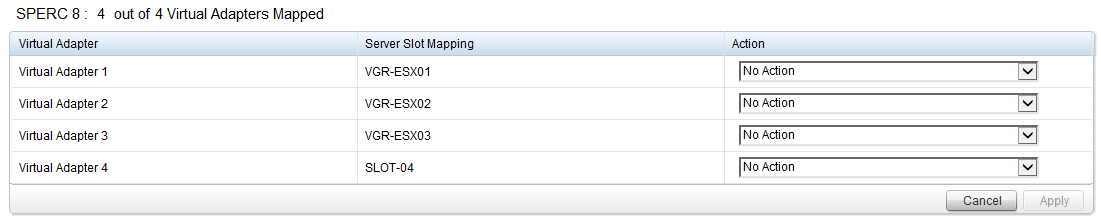
Installing ESXi (repeat for each blade):

* Verify that the VRTX’ shared storage has **not** been assigned to the blades. **Caution**: if they are assigned, they will be wiped.
* During booting of the blade verify that the local raid controller of the blade has configured 1 raid array (both disks in RAID 1). This is the standard Dell configuration and is expected for all clean installs.
* Plug the USB stick into the blade (not the VRTX), enter the boot menu and select the USB stick as boot source in the BIOS. It is recommended to use BIOS, not UEFI.
* If you booted from BIOS, you will see a boot menu showing multiple options. This will not occur if you chose UEFI. The boot menu will include the 3 configured .cfg files included on the USB stick. Select the correct cfg based on the blade’s slot.
* Once an option has been selected, the installer will kick off the install. During the install, the server will need to reboot. Do not remove the USB after this reboot. It is still needed to complete the configuration after reboot.
* Once the configuration has been completed, the server will display the ESXi’s Direct Console User Interface (DCUI). Log in by pressing F2 and entering the username (root?) and password as configured in your kickstart configuration files. Verify that your configuration was correctly applied.

Configure shared storage:

* In the CMC, under “Chassis Overview” > “Storage” and the Setup tab, map the virtual adapters to the relevant blades.





* In “Chassis Overview” > “Storage” > “Virtual Disks” under the “Assign” tab, now grant “Full Access” to one blade. This blade should be the one referenced in the configuration.xml of your deployment scripts. It will be the blade to which you will push the vCenter. Once the other ESX servers have been added into the vSphere cluster in later steps, the shared storage can be assigned to them as well. This is something which will be done later, since doing it at this stage can generate issues during the automatic creation of the cluster.
* Configure shared storage (to be executed exclusively on the first ESX server):
  + Connect to the first ESX server using your vSphere Client (aka the “vSphere C# Client”).
  + Go to the “Configuration” tab > “Hardware” > “Storage”.
  + Click “Rescan all”.
  + Click “Add storage...”.
  + Select the disk with the storage path id containing “T0”.
  + Use VMFS-5.
  + Name it “VirtualDisk1R6”.
  + Use all available space to create the datastore.
  + Repeat steps for “T1” (as VirtualDisk2R6), “T2” (as VirtualDisk3R6), etc until all available disks contain a new datastore.
  + Note: Be careful, for scripts to work the names of the virtual disks need to be exactly correct. Example below for the 16x 600GB configuration:
    - VirtualDisk1R6: 1.50 TB (used for the vCenter, DC & templates)
    - VirtualDisk2R6: 1.50 TB (used for servers)
    - VirtualDisk3R6: 1.50 TB (used for clients)
    - VirtualDisk4R6: 2.04 TB (used for the file server)

# Dell storage performance tweaks

In this section we will execute some VRTX specific performance tweaks. These tweaks will need to be applied on each ESXi server separately. Only applying them on a single ESXi can cause serious performance issues on the cluster.

Step by step procedure to be executed on each ESXi host:

* Connect the vSphere Client to the ESXi host.
  + In the “Inventory View”, select the host. Then select the “Configuration” tab. In the sidebar select “Software” > “Advanced Settings”.
  + Select “Disk” in the sidebar and scroll to Disk.DiskReservationThreshold and set the value to “1”.
* Open Putty and connect to the ESXi host.
  + Once connected, run “esxcli storage core device list”. This will display a list of storage devices. For all “DELL Serial Attached SCSI Disk” devices, copy the “naa.” identifier. Local disks should be ignored. The number of naa.identifiers which you need to copy equals the number of shared virtual disks created on the VRTX.
  + Now run “esxcli storage core device set --device <naa.idenfitier> --queue-full-sample-size 32 --queue-full-threshold 8 --sched-num-req-outstanding 128” where the <naa.idenfitier> is the value noted above. The command will provide no output. To verify correct execution, run “esxcli storage core device list” and verify that the following parameters are set for the “DELL Serial Attached SCSI Disk” devices:
    - Queue Full Sample Size: 32
    - Queue Full Threshold: 8
    - No of outstanding IOs with competing worlds: 128

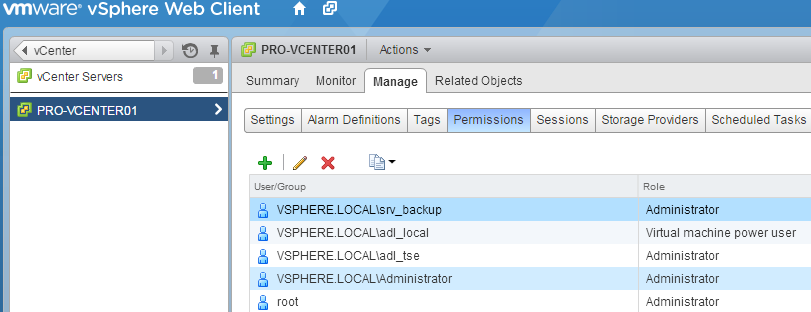
# VMWare vCenter appliance

In this section we deploy the VMWare vCenter appliance ova/ovf template to the shared storage of the first ESXi servers. The configuration is largely automated, but some steps cannot be scripted in version 5.5.

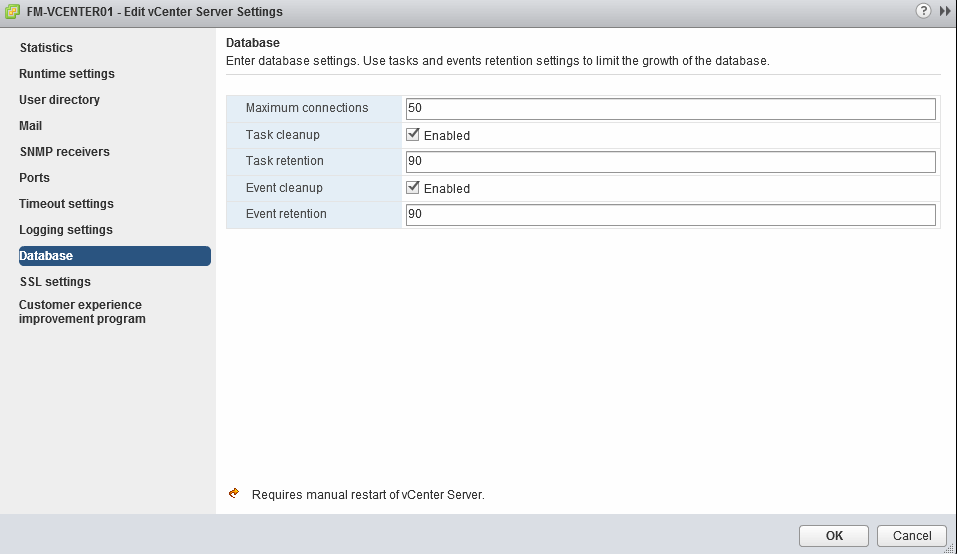
Once networking is set up, the appliance management interface can be accessed by surfing to its IP using https & port 5480. The settings in this interface will most likely not need to be changed. Most configuration will be done through the vSphere Web Client: https://<IP>:9443/vsphere-client/

Step by step deployment procedure:

* Execute your local copy of ...\Scripted Install\Scripts\StartThisElevated.ps1 while elevating the script (run PowerCLI as administrator).
* You will be shown a numbered menu and an overview of the currently configured variables which will be used for the install.
* Pick the “*Deploy vCenter*” menu option and press enter.
* The vCenter appliance will be deployed using your previously edited configuration. This will include adding the configured ESX servers into a cluster.
* Verify that the other servers have been added to the cluster by logging into the vCenter’s vSphere Web Client. For this, use the [administrator@vsphere.local](mailto:administrator@vsphere.local) user, since you will need the SSO administrator for steps further down. The root user does not have rights to see or modify SSO groups.
* When all ESXi servers have been added to the vSphere cluster, you should now assign the virtual adapters of the shared storage to all ESXis (blades) in the CMC as you have already done for the first blade. This is done in “Chassis Overview” > “Storage” > “Virtual Disks” under the “Assign” tab.
* Back in the vSphere (Web) client, discover the shared storage (for each ESX server):
  + Select each host server
  + Go to the “Configuration” tab > “Hardware” > “Storage”.
  + Click “Rescan all”.
  + You should see storage appear on each of the servers.
* Configure the Single Sign-On policies:
  + Go back to the home page of the vSphere Web Client. Click “Administration” on the menu bar.
  + Under “Administration” > “Single Sign-On” > “Configuration”, click tab “Policies” and then “Password Policies” & Edit. Configure:
    - Description: “JDN policy”
    - Maximum lifetime: 9999 days
    - Restrict re-use: 1 passwords
    - Maximum length: 20
    - Minimum length: 10
    - Characters: At least 0 special characters, 2 alphabetic, 1 numeric, 1 lower case, 1 upper case.
  + Now click “Lockout Policy” & Edit. Configure:
    - Description: “JDN Policy”
    - Max failed attempts: 10
    - Time interval between failures: 10 minutes
    - Unlock time: 10 minutes
* Configure the Single Sign-On domain:
  + Under “Administration” > “Single Sign-On” > “Configuration”, click tab “Identity Sources”.
  + Select the line with “vsphere.local”.
  + Click “Set as Default Domain”.
  + This will allow “[administrator@vsphere.local](mailto:administrator@vsphere.local)” to log in as “administrator” instead. This also makes it easier for users which we will create in the vsphere.local SSO domain. However, the “root” account will now need to log in with “root@localos”.
* Create a new Access Control role:
  + Under “Administration” > “Single Sign-On” > “Access Control” > “Roles”, select the line with “Virtual machine power user (sample)”.
  + With the line selected, click the “Clone role action” icon.
  + Name the new role “Virtual machine power user”.
  + Right click the new role and click “Edit”.
  + Under “Host” > “Configuration”, check the checkboxes for “Maintenance” & “Power”.
  + Press “OK”.
* Configure the Single Sign-On users:
  + Under “Administration” > “Single Sign-On” > “Users and Groups”, click tab “Users”.
  + Make sure Domain “vsphere.local” is selected.
  + Click the + sign to create a local user:
    - User name: adl\_local
    - First name: ADL
    - Last name: Local
  + Click the + sign to create a TSE user:
    - User name: adl\_tse
    - First name: ADL
    - Last name: TSE
  + Click the + sign to create a backup service user:
    - User name: srv\_backup
    - First name: Service User
    - Last name: Backup
  + Click the + sign to create a backup service user:
    - User name: srv\_ups
    - First name: Powerchute
    - Last name: UPS
  + Click the “Groups” tab.
  + Select the “Administrators” group.
  + In the “Group Members” pane, click the + sign to add users to the group.
  + Add “adl\_tse”, “srv\_backup” & “srv\_ups” users and click OK.
* Assign Permissions:
  + Go to the vCenter server, select the “Manage” tab and then the “Permissions” button.



* + Click the + sign to add a user.
    - Click “Add...” under the “Users and Groups” section and enter:
      * Domain: VSPHERE.LOCAL
      * User/Group: adl\_local
      * Click “Add”.
      * Click “OK”.
    - Select “Virtual machine power user” from the drop down under “Assigned Role”. Make sure NOT to select the “sample” role.
    - Click “OK”.
  + Click the + sign to add a user.
    - Click “Add...” under the “Users and Groups” section and enter:
      * Domain: VSPHERE.LOCAL
      * User/Group: adl\_tse, srv\_backup & srv\_ups
      * Click “Add”.
      * Click “OK”.
    - Select “Administrator” from the drop down under “Assigned Role”.
    - Click “OK”.
  + Change the vCenter retention policy.
    - Go to the vCenter server, select the “Manage” tab and then the “Settings” button and “Edit”
    - At the database settings
      * Check “Task cleanup” and set task retention to “90”
      * Check the “Event cleanup” and set the event retention to “90”



# Template/OVA deployment

In this section we deploy the OVAs which were present on the network share and convert them into ready to use templates.

Step by step deployment procedure:

* If you do not have the script already running, execute your local copy of ...\Scripted Install\Scripts\StartThisElevated.ps1 while elevating the script (run PowerCLI as administrator).
* You will be shown a numbered menu and an overview of the currently configured variables which will be used for the install.
* Pick the “*Deploy OVAs*” menu option and press enter.
* The OVAs will be deployed and subsequently converted to templates.
* Verify that the necessary templates were made available.

# DC deployment

In this section we deploy the domain controller OVA and configure the domain.

Step by step deployment procedure:

* If you do not have the script already running, execute your local copy of ...\Scripted Install\Scripts\StartThisElevated.ps1 while elevating the script (run PowerCLI as administrator).
* You will be shown a numbered menu and an overview of the currently configured variables which will be used for the install.
* Pick the “*Deploy Domain Controller*” menu option and press enter.
* The DC OVA will be deployed.
* The VM contains a number of configuration scripts that can be run to configure the domain automatically. However, you should always retrieve the latest DC configuration scripts from Meso. Consult the other documentation to learn more about the DC configuration steps and do not forget to execute them before continuing.
* Note: Be sure to wait long enough before executing the install & configure scripts. Your VM needs to reboot to run the customization script which is deployed together with your VM.

For detailed description of DC configuration, please consult <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed825acff1>

More information on the XML structure for creating shares etc can be found in <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed825a7474>

# VM deployment

In this section we deploy a number of VMs, put them in the right folders and where possible join them to the available domain.

Step by step deployment procedure:

* If you do not have the script already running, execute your local copy of ...\Scripted Install\Scripts\StartThisElevated.ps1 while elevating the script (run PowerCLI as administrator).
* You will be shown a numbered menu and an overview of the currently configured variables which will be used for the install.
* Pick the “*Deploy VMs*” menu option and press enter.
* VMs will now be deployed & started. Keep in mind that joining them into the domain (if available) can take up to 15 minutes after deployment. To join the domain, they will restart automatically. Please do not interrupt their configuration until they have joined the domain (if applicable).
* After the script has completed, you can begin manually deploying additional VMs as required by your specific environment.
* Once the VMs have joined the domain, do not forget to move them to the correct OUs in Active Directory and to enable time synchronization via the VM Tools (under “Edit VM Settings” > “VM Tools” > “VM Tools”) where applicable. Warning: The DC should NEVER synchronize time through VM Tools.
* Your MGMT01 VM will have 2 NICs, only one of which has an IP assigned. You can manually configure the second NIC as:
  + IP: 172.16.3.20
  + Mask: 255.255.255.128
  + Do not configure a gateway or DNS on this NIC
* Once all the VMs have joined the domain, now run the “Finalize Deployment” option of the PowerCLI script. This will set the time zone to UTC, as is standard for ships. For offices & sites, using UTC is allowed, but other time zones can be configured. To do this, modify the $timeZone variable in the $SETTIMEZONESCRIPT string. Be careful, “CET” is not a valid entry. You need to use the syntax found in tzutil.exe /l. Example: “CET” translates to “Romance Standard Time”.
* Currently Windows 7 client VMs are rolled out with only a 5 GB D:\ partition. It is allowed to extend this partition up to 20 GB for the captain, chief & elec VMs. Extending this partition should be avoided for all other VMs.

# ISO deployment

Go to the first shared datastore using your vSphere client or vSphere Web client. Create a new folder named “ISO”. Manually upload the useful ISOs available in ...\Software\Current\ to the datastore. It is especially important to upload the Windows ISOs.

# Manual deployment of additional VMs

Additional VMs can be deployed as documented in <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed81c55abc>

# Synology NAS configuration

See: <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed81d46020>

# UPS configuration

See <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed81c55af7>

# Veeam backup configuration

See <http://meso.jandenul.com/meso-webtop/drl/objectId/090236ed81c55b22>

# Other useful documentation

See

<http://www.dell.com/support/home/us/en/19/product-support/product/poweredge-vrtx/manuals?c=us>

<http://meso.jandenul.com/meso-webtop/drl/objectId/0b0236ed81a9b985>