

Please make sure the xx-monitor01 server has full internet access during this installation to ensure the License activation can be completed.

# PRTG software installation on server

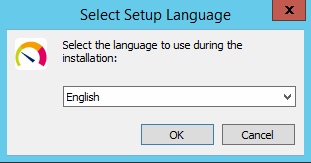
## Expand virtual harddisk

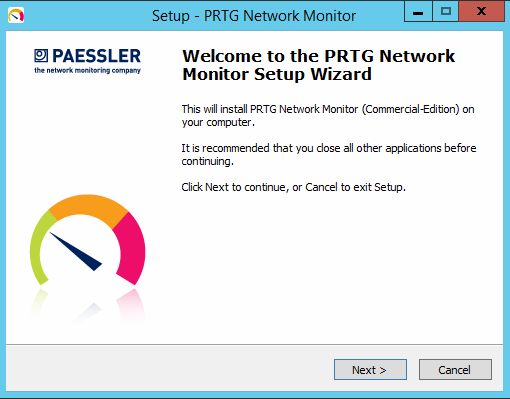
Expand the virtual harddrive of your xx-monitor01 VM to 200GB, reboot the VM and expand in disk management.

## Files to copy to your PRTG server

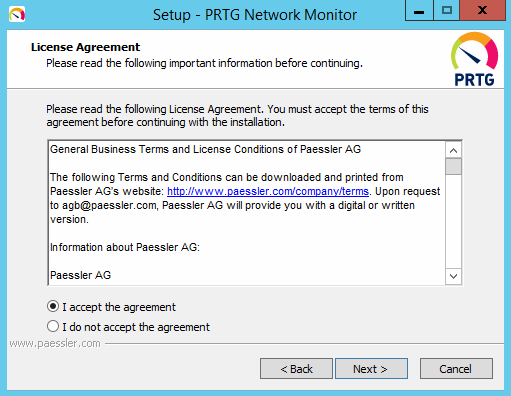
* PRTG Latest package can be found on: [\\jdn-file01\software$\Software - Windows Official\PRTG Network Monitor](file:///\\jdn-file01\software$\Software%20-%20Windows%20Official\PRTG%20Network%20Monitor\)
* Copy the following subdirectories to xx-monitor01:
  + PRTG - Configuration Files **From TFS**
  + PRTG - Vessel
  + PRTG - Software
* License file can be found on the IT intranet (http://vm-web02/)

Run \PRTG - Software\PRTG Network Monitor 1X.X.X.XXX.exe

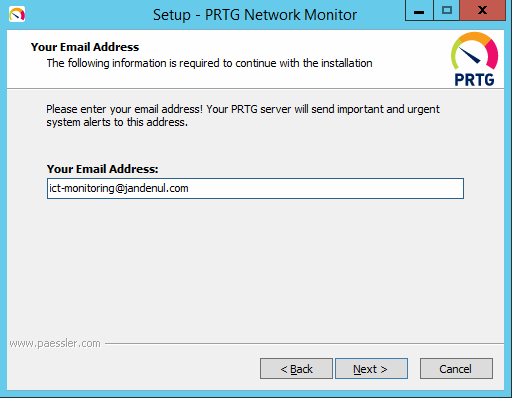




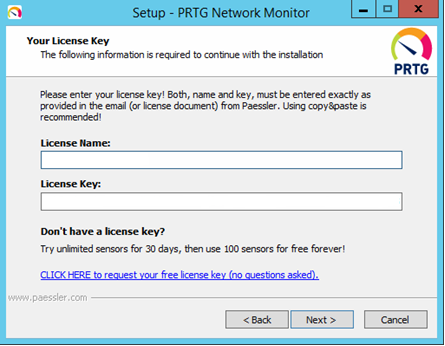
* Select ‘English’ and click ‘OK’
* Click ‘Next’

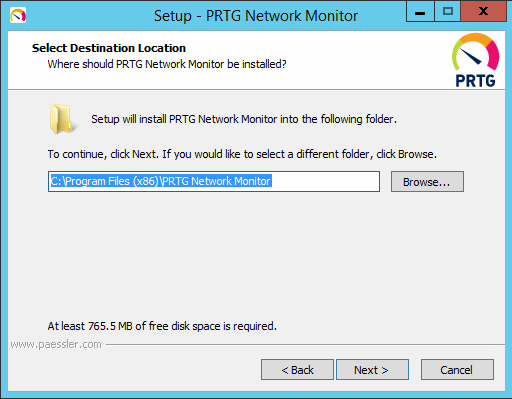


* Select ‘I Accept the agreement’ and click ‘Next’



* Fill in ‘ict-monitoring@jandenul.com’ and click ‘Next’



* Fill in the Name and License (check IT intranet vm-web02.jandenul.com)
* Click ‘Next’  
    
  
* Leave default installation Path and click ‘Next’

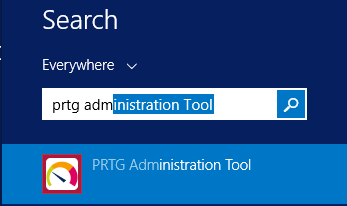
# PRTG Configuration

## Copy installation files to correct directory

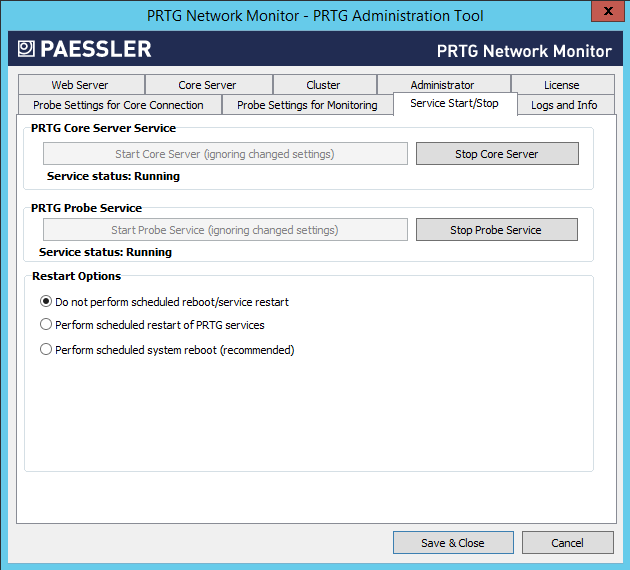
* Copy the contents of the PRTG install Files folder to: C:\Program Files (x86)\PRTG Network Monitor (append).

## Change Template Configuration file

* Open the PRTG - Configuration Files directory you copied in the first step of this manual
* Run the PowerShell script and follow the steps on the screen to generate a config file for your PRTG installation. Name the exported file 'PRTG Configuration.dat'
* Open PRTG Administation tool



* Go to tab Service Start / Stop

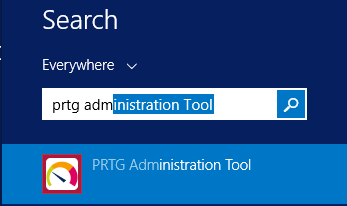


* Stop core server and probe service
* Copy newly created configuration file to C:\ProgramData\Paessler\PRTG Network Monitor
  + Copy and replace
* Start core server
  + Do not start the Probe Service

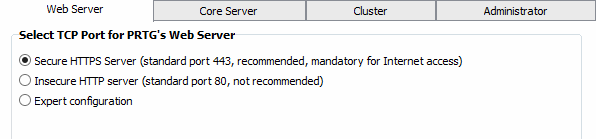
## Extra configuration

### HTTPS encryption

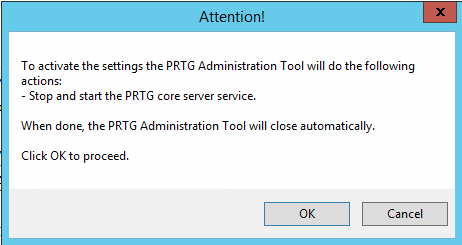
* Open PRTG Administation tool



* Go to tab ‘Web Server’
* Change Insecure HTTP to Secure HTTPS server



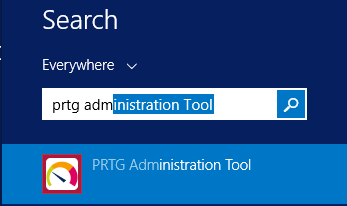
* Click Save & Close
* Click OK



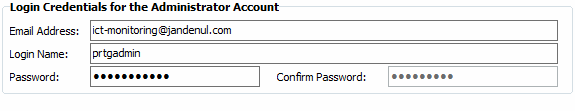
* PRTG will now restart all services

### Prtgadmin password

* Open PRTG Administation tool

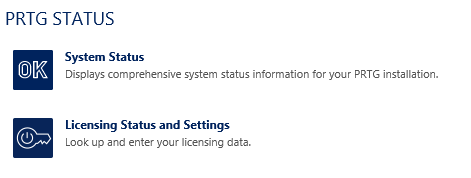


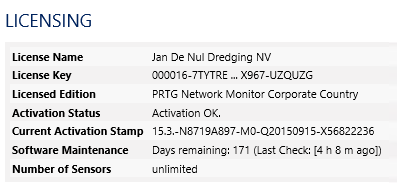
* Go to tab ‘Administrator’



* new password: XXprtg”amosnumberofvessel” or “project code” (ex. VDprtg085)
* Click ‘Save & Close’
* Click ‘OK’
* PRTG services will now restart >> Make sure the Probe service is not running
* Add the user and password to Remote desktop manager.

## Activation

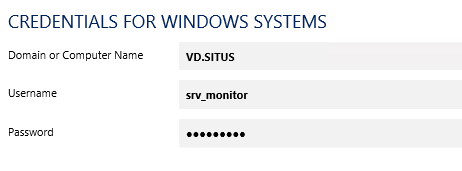
* Browse to <http://10.xxx.xxx.25> (use chrome or firefox on your management VM) and login with prtgadmin and newly created password.
* To check if activation is successful Go to Setup 🡺 PRTG Status 🡺 Licensing Status and Settings  
  
* Check if Activation Status is Activation OK. (if not check internet connection and restart services)



## PRTG Settings

### Credentials for Windows Systems

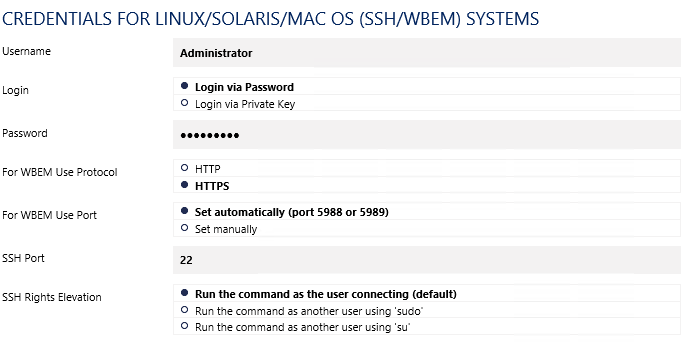
* Change following settings



* NetBIOS Domain Name
* Username
* Password

### Change Linux/Solaris/MAC OS (SSH/WBEM)

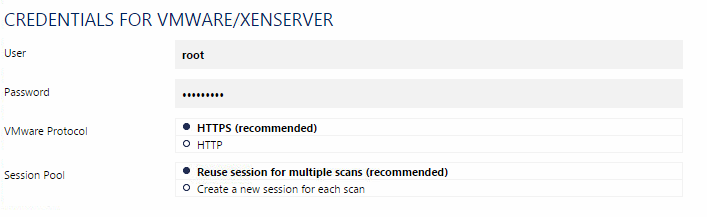
* Change following settings



* + Username
  + Password

### Change VMWare/Xenserver

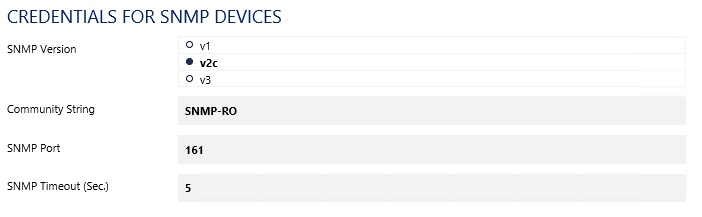
* Change following settings



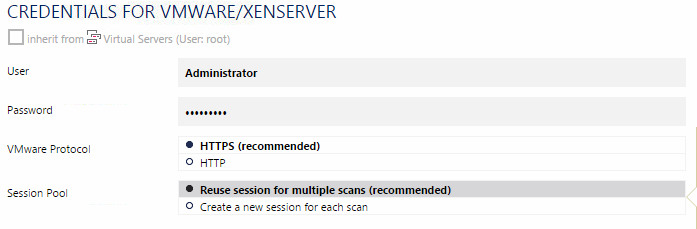
* + User
  + Password

### Credentials for SNMP devices

* This setting should be ok but check to make sure.



* SNMP-RO
  + Every device that is going to be monitored with PRTG through PRTG should get the appropriate SNMP string and version (if possible).
* Select the xx-vcenter01 device
  + Click Tab ‘settings’
  + Go to ‘Credentials for VMWARE/XENSERVER’ and uncheck the inheritance

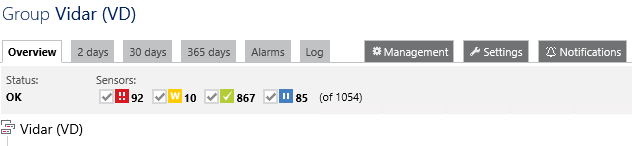


* + Fill in correct password

**Start the Probe service**

### General Settings

* Rename 127.0.0.1 probe name to xx-monitor01.xx.situs
* Click on Vessel Name (XX)
* Go to ‘Settings’

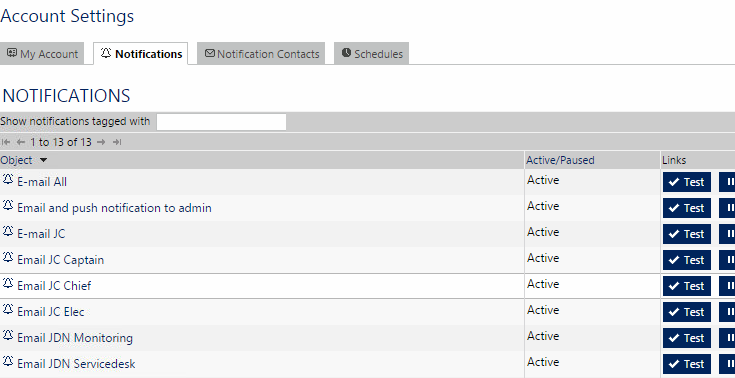


### Notification

* Please make sure commbox user [monitoring@xx.jandenul.com](mailto:monitoring@xx.jandenul.com) has been created in the commbox. (webmail rights)

For sites, make sure you use srv\_prtg\_<site>@jandenul.com

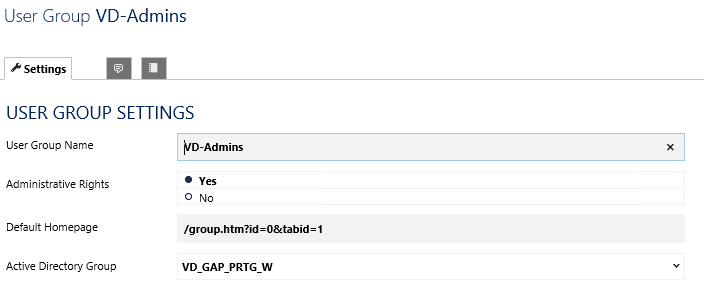
* Go to Setup 🡺 Notifications



* Next to E-mail “test” edit and fill in your own email address and test if you receive the mail

### Users

* Go to Setup
* User groups
* Open XX-Admins and check that Active Directory Group is correct (XX\_GAP\_PRTG\_W) otherwise change this.



* Open XX-Users and check that Active Directory Group is correct (XX\_GAP\_PRTG\_R) otherwise change this.

# Setting up remaining Devices and sensors

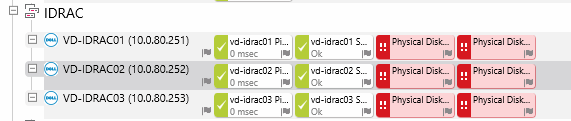
## Firewall (XX-FW01)

## CMC (Not DL20)

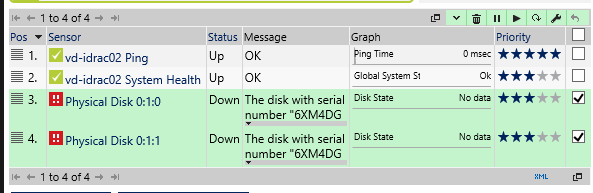
* Select the XX-CMC01
* Go to tab ‘Settings’
* Unbreak inheritance for SNMP credentials

## IDRAC Sensors (Not DL20)

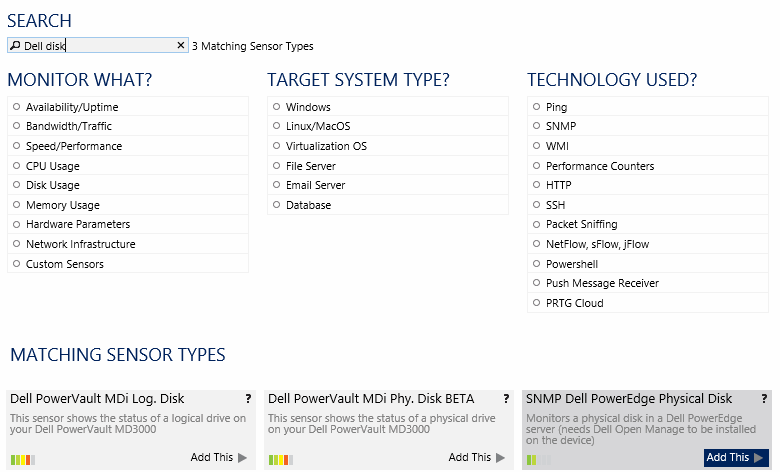
* Physical disk sensors will not work due to different serial numbers so they will have to be re-added.



* Select the IDRAC and select the physical disk sensors



* + Click the delete icon
* Click Add Sensor
  + search Dell disk



* + Add SNMP Dell Poweredge Physical Disk
* repeat these steps for all IDRAC’s

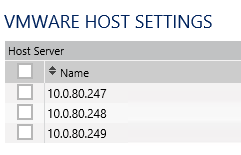
## Commbox

* Select the xx-commbox01 device
* Select the IMAP sensor and select the Settings tab
* Change the password for the monitoring account

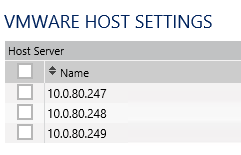


## vCenter

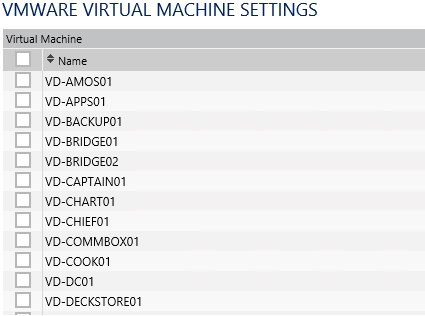
* Remove all sensors except for Ping
* Add new sensor VMware host Performance (SOAP) (check option Virtualization OS)
  + Check all hosts



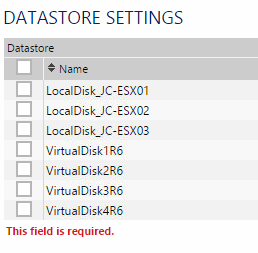
* Add new sensor VMware host hardware Status (SOAP)
  + Check all hosts



* Add new sensor VMware virtual machine (SOAP)
  + Check all virtual machines

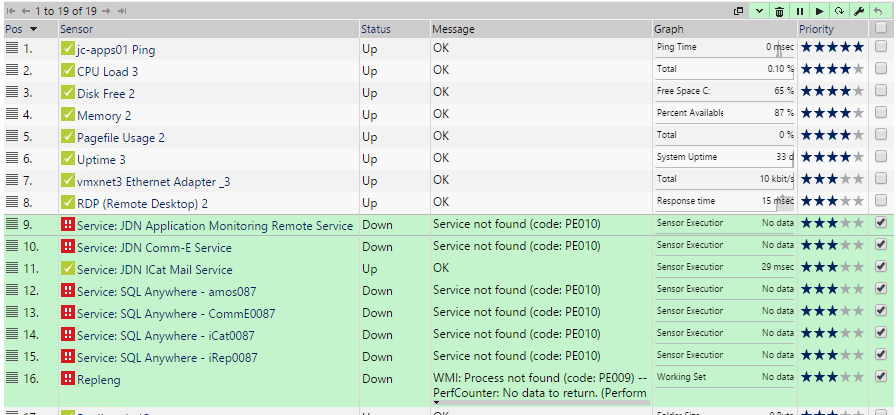


* Add new sensor VMWare Datastore (SOAP)
  + Check all datastores

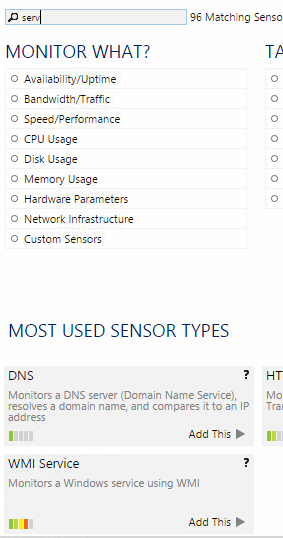


## Xx-apps01

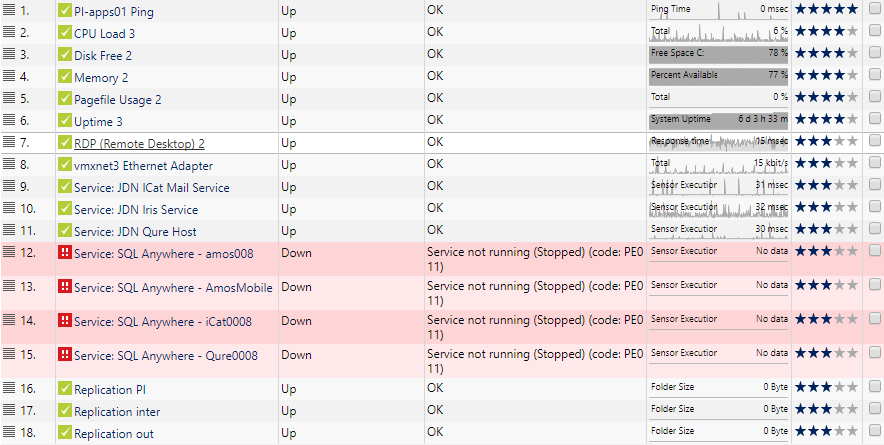
* Select the xx-apps01
* Remove existing services



* Add sensor WMI service



* Select all relevant JDN Services



## Timeserver

* Select the XX-TIME01
* Go to tab ‘Settings’
* Unbreak inheritance for SNMP credentials

If this is not used please delete this entry.

## Survey storage

If this is not used please delete this entry

## Serial server

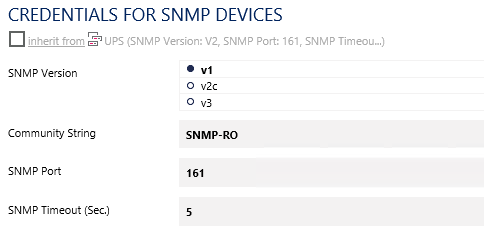
If this is not used please delete this entry

## Network (NOT DL20)

* Remove all extra switch nodes except for node 0
* Rename xx-SW01 node 0 to xx-SW01
* Remove all SNMP traffic sensors
* Add sensor 🡺 SNMP Traffic 🡺 Check all

## UPS (do this if it doesn’t work)

* Select the group UPS
* Click the settings tab
* Uncheck the ‘Credentials for SNMP Devices’ to disable the inheritence.
  + Switch SNMP version to v1

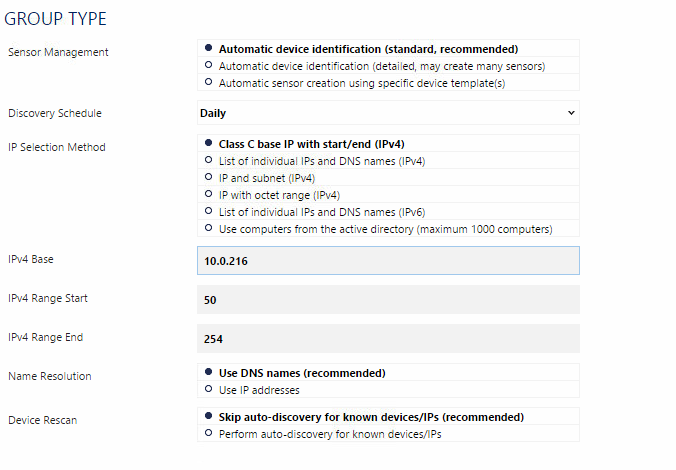


## WLAN

* Select XX-WLAN01
* Check SNMP traffic sensors that are down
* Re add those SNMP traffic sensors

## Admin-Trust Autodiscovery group

* Rightclick the xx-monitor.xx.situs node and click on ‘Add Auto Discovery Group’
  + Group Name: Admin-Trust DHCP
  + Discovery Schedule: Daily
  + IPv4 Base: Admin trust IP base 10.xxx.xxx
  + Start: 50
  + End 254

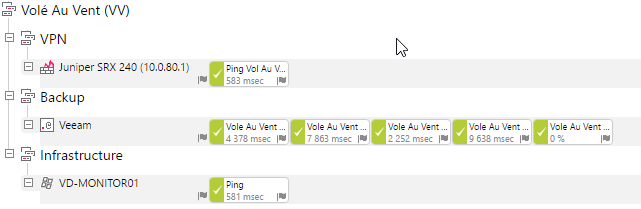


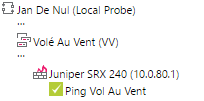
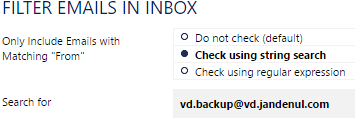
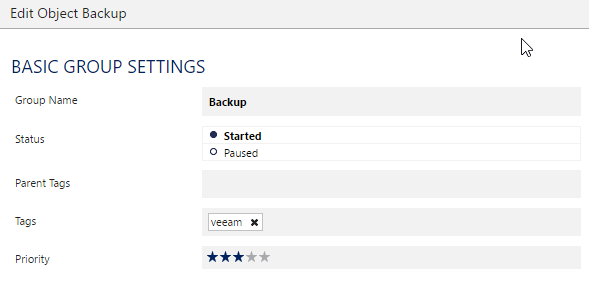
# Change JDN PRTG

## JDN-PRTG02

Login to <https://jdn-prtg02.jandenul.com>

Clone the following devices from **Volé Au Vent (VV)** to your Vessel/Office device.



* Juniper SRX 240 (10.0.80.1)
  + Change the juniper model if needed.
  + Change the ip-address to you firewall ip-address
  + Change the name of the ping sensor to “Ping <vessel/office name>
* VD-MONITOR01
  + Change the device name to your vessel/office abbreviation XX-MONITOR01
  + Change the IPv4 address
  + Change the Dependency to the ping sensor of the Juniper SRX 
* Backup
  + Change the imapsensor name with the vessel/office name
  + Change the “Filter emails in inbox > search for” to your vessel/office abbreviation 
  + Add the “veeam” tag to the Backup group

If the new setup is already in production. Cleanup all the old sensors. If the old setup is still in production, remove them after the swap.

# Snapshot Search Script

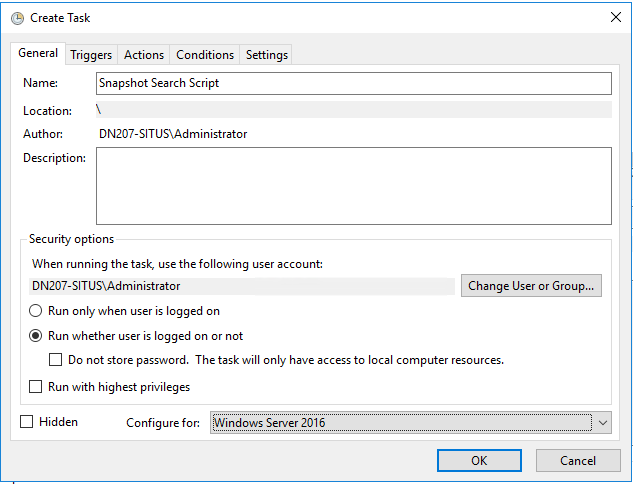
Copy the latest versisio of the script from: **\\Jdn-file01\ict\_new\_standard\_sites\_vessels\Other\Check for snapshots** to XX-MONITOR01 **C:\Program Files (x86)\JDN\Operations**

Edit the script variables with the parameters of the vessel

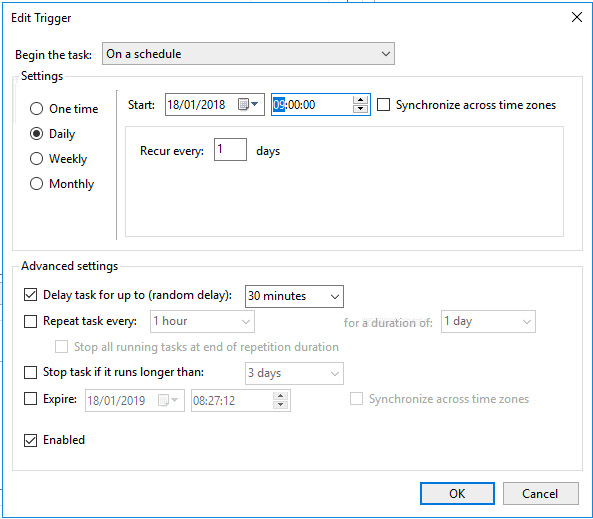


Add the vcenter credentials with Powershell (command will only work when PowerCLI is installed):  
**New-VICredentialStoreItem -Host 10.X.X.10 -User 'administrator@vsphere.local' -Password 'password'**

Create a new Scheduled task.



Create a new Trigger



Create a new Action

Arguments:   
**-ExecutionPolicy Bypass -File "C:\Program Files (x86)\JDN\Operations\SnapshotSearchReport.ps1"**

