

Install and Configure Lefthand Networks VSA (SAN/IQ)

*A sample chapter from my forthcoming
book on VMware's Site Recovery Manger*

RTFM Education

Beyond the Manual... with Mike Laverick

By Mike Laverick
© [RTFM Education](#)

For Errors/Corrections please contact:
mikelaverick@rtfm-ed.co.uk

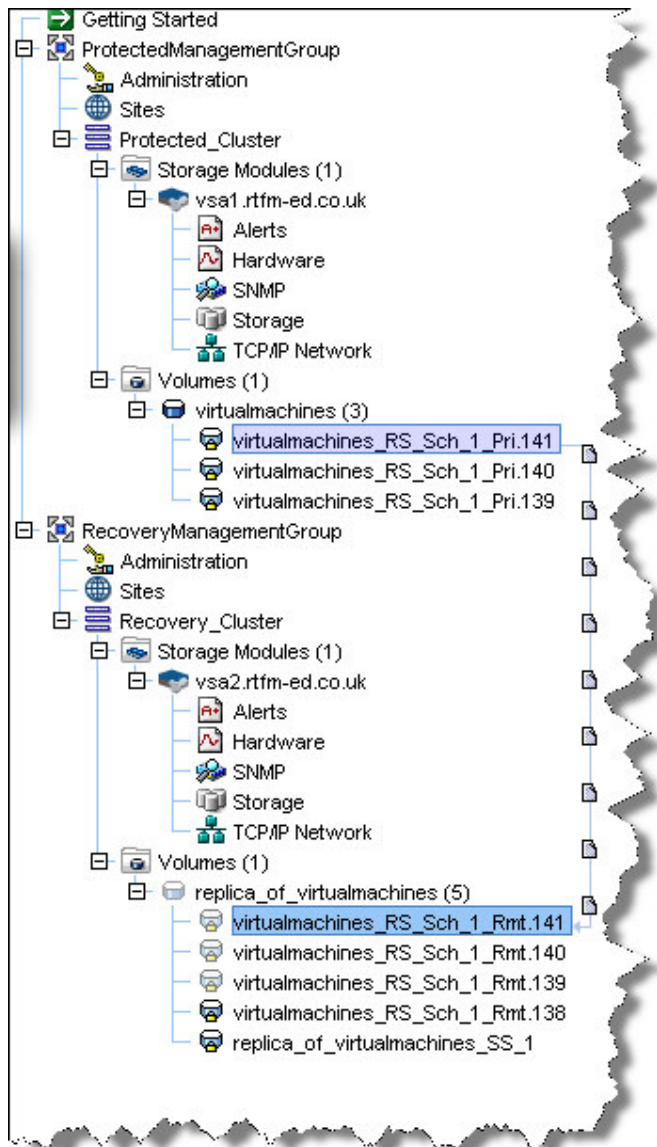
SAMPLE - NOT FOR RESALE/EPK

SAMPLE - NOT FOR RESALE/REPRODUCTION

Chapter 2: Getting started with Lefthand Network's VSA Virtual Appliance

Note:

LeftHand Networks are a company that provides both physical and virtual storage IP based appliances in the iSCSI SAN market. In particular they have virtual appliance called the VSA which is downloadable from their website for a 30-day evaluation period. In this respect its ideal for any jobbing server guy to download and play with in conjunction with SRM. If you follow this guide to the letter you should end up with a structure that looks like this in the VSA's management console, with the friendly names adjust to suit your own conventions.



Some Frequently Ask Questions about LeftHand Network's VSA

- 1. What are the recommend minimums for memory and CPU?**
1GB RAM, 1 vCPU offering 2Ghz of CPU time or larger. The adding of additional vCPUs does not significantly improve performance
- 2. Should the VSA be stored on a Local VMFS volume OR a Shared VMFS volume?**
Depends entirely on the quality of the storage. If you local storage is faster and offers more redundancy that any remote storage you have – then you would use local storage. In some environments you might prefer to use shared storage to facilitate backup, deployment, and allow for redundancy/performance with VMware DRS/HA
- 3. VSA is licensed by MAC address – should you use a static MAC address?**
It is recommended to use a static MAC address if you decide to purchase the VSA. If you are just evaluating VSA or simply using it to evaluate SRM it is not required, just recommended
- 4. Can you use VirtualCenter cloning to assist in creating multiple VSAs?**
Yes. But the VSA must not be configured or in a management group. If you have procured a licensed version of VSA be aware that that template deploy process generates a new MAC address for the new VM, as such will need licensing or relicensing after being deployed
- 5. Setting up two VSAs in a management group with all the appropriate settings takes some time. Can you use the clone feature in VirtualCenter to reset lab environments?**
Yes, simply right-click the Management Group – and choose the option to Shutdown Management Group. You can then clone, delete and re-clone again. The cloning process does not change the MAC address but, the template process does. An alternative to this approach is to learn the Lefthand Networks CLI which allows you to script this procedure. This is not covered in this guide.
- 6. Can you capture the configuration of the VSA's and restore it?**
Yes and No. You can capture the configuration for support purposes but not for configuration. Future versions of the VSA may have this ability. Perhaps capturing the configuration to an XML file which would allow for its reloading. This would stop the need to clone or script the high-level configuration process that occurs in the Management Console

Download and Upload the VSA

Currently, the VSA is not in the downloadable "Open Virtual Machine Format" (OVF). Instead you download it as a ZIP file, and then upload and extract on your ESX host. The ZIP file contains a virtual disk file and other files that make up a virtual machine, but these other files are not compatible with ESX 3.5. So you will have to make a new VM, and point the virtual machine to the VSA virtual disks. The VSA runs on a Linux kernel and will use Other Linux (32-bit) as its virtual machine type. Anyway, let's cut to the chase – let me take you through that process. In the meantime you might as well begin downloading the VSA from here:

<http://www.lefthandnetworks.com/products/vsa.php>

There is a blog, forum and PDF guide available on the site as well.

Create the VSA Virtual Machine

1. **Right-click** your **ESX host**
2. Choose **New Virtual Machine**
3. Choose **Custom**
4. **Type in a name for your VSA** such as **vsa1.rtfm-ed.co.uk**

Note:

You will have to create two VSAs as that's kinda requirement to have both replication or snapshots for DR/BC configuration! ☺

5. Choose a **Local VMFS Volume**

Note:

I've opted used local storage as opposed to my SAN. The SAN I have is quite old, slow and I have limited disk space. This virtual appliance is going to have some overhead attached to given that it will run as VM on VMFS volume offering up LUNs (which are in fact virtual disks) to ESX hosts, which in turn will format those as VMFS volumes to store other VMs. That's right I'm going have a VMs stored within another VM. VSA wasn't designed for this purpose although it does work. I thought putting my VSA on local storage would be best for reducing any virtualization overhead on the disks, and because I have plenty of free local disk storage

6. Choose **Linux** and **Other Linux (32-bit)** as the Guest Operating System
7. Choose **1-vCPU** and at least **1GB** of RAM
8. **Attach the VM to a port group**

Note:

This will need to be accessible from your other ESX Hosts. If you are using the Software iSCSI Initiator like I will remember you also need both a vmkernel port group and service console port group to access the iSCSI appliance

9. Select **LSI Logic** as the **virtual SCSI Controller** for the VM
10. Choose **Do not create disk**

Note:

We will be shortly unzipping and extracting the downloaded files to the directory created by process above, and attaching them to the VSA VM.

Extract the VSA ZIP File

The VSA contains a number of files but we only require the virtual disks. I uploaded my VSA zip to the SAN for further use and to centralize its storage.

You can extract the VSA virtual disk files using the Service Consoles ZIP utility like so:

```
unzip /vmfs/volumes/isos/lefthand-networks-activate-vsa_esx.zip *.vmdk -d /vmfs/volumes/esx1\storage1/vsa1/
```

Note:

Here I'm extracting just the VMDK files from the zip with *.vmdk -d. The source is my ISOs datastore and the destination is the virtual machine directory of /vsa1

Add the Virtual Disks

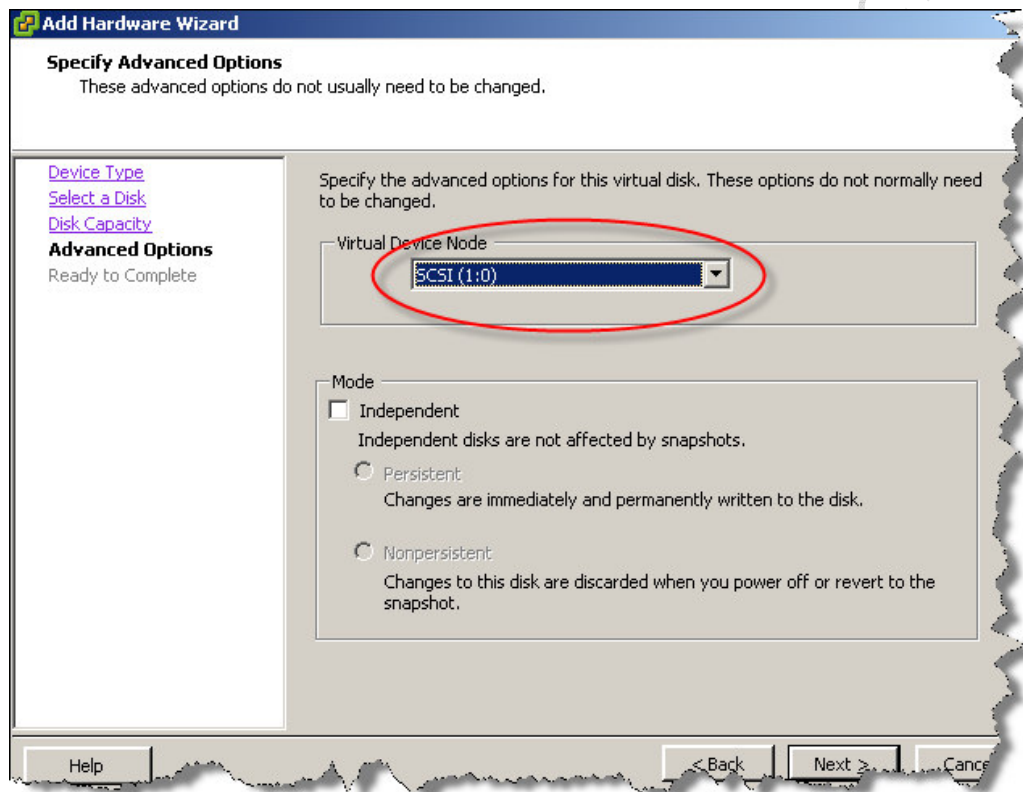
1. **Right-click** your VSA

2. Select **Edit Settings**
3. Click the **Add** button to add hardware
4. Select **Hard Disk** as the type
5. Choose **Existing Disk**
6. Select the first disk named, **VSA.vmdk**
7. Select **SCSI 0:0** as the **location as this is the boot disk**

Note:

Repeat this for the second virtual disk called VSA_1.vmdk but this time attach it to SCSI 0:1

8. Next **add in a third and final disk**. This disk will be volume presented to your ESX hosts. As such you will want to make it as big as possible as you will create VMs here. **Additionally it must be located on SCSI 1:0**



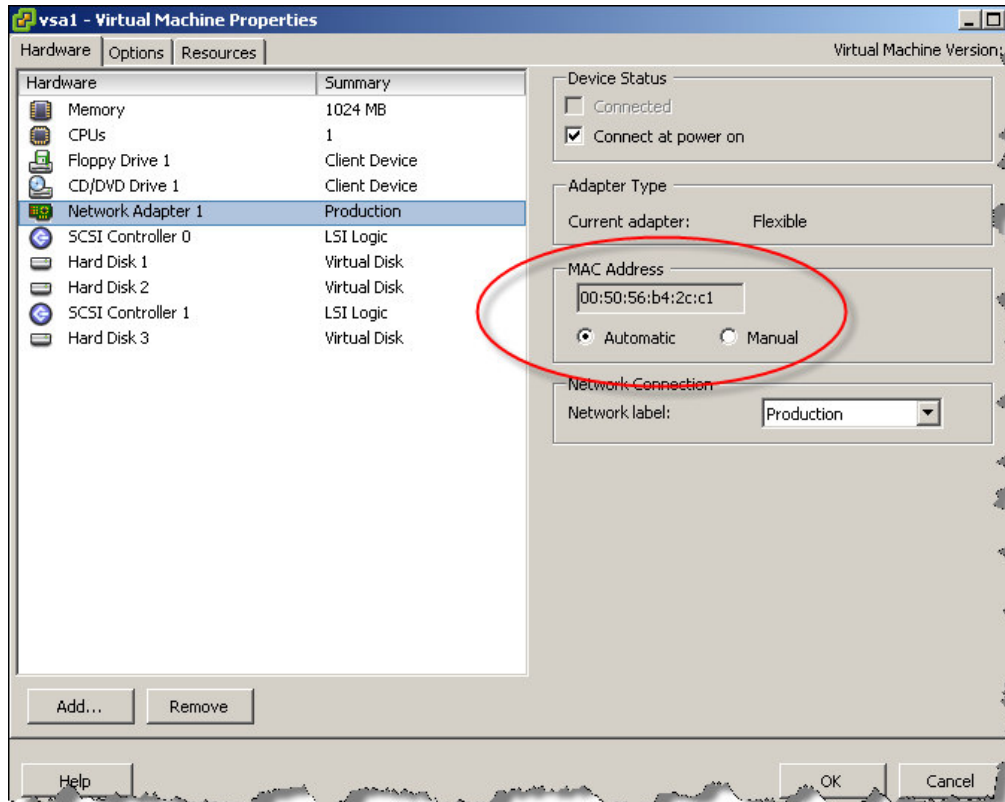
Note:

Later when we create volumes in the VSA, I will use "thin provisioning" to present this disks a 1TB LUN. Despite doing this – the larger this third disk is the more space you will have for your virtual machines.

Licensed by Virtual MAC Address

Before you power on the VSA for the first time, you might want to consider how the product is licensed should you wish to use VSA beyond the 30-day evaluation period. VSA is license by the virtual MAC address of the VM generated by VMware at power on. Whilst this auto-generated MAC address shouldn't change, it can do in some case where you register and unregister a VM from one ESX host to another. Additionally, if you fail to back up the VMX you could lose this information for ever. Lastly, if for whatever reason you clone the VSA with VirtualCenter clone/clone to template facility, a brand-new MAC address is generated at that point. To be 100% sure you might prefer to set

and record a static MAC address to your VSA. It depends on your circumstances and requirements. If you wish set a static MAC address in the range provided by VMware. Since Vi3.5 you have been able to set a static MAC address



Whatever you chose static or dynamic – be sure to make a record of the MAC address so your license keys (if you have purchased one) can be used if you want to completely rebuild the VSA from scratch. Lefthand Networks recommend a static MAC address.

Primary Configuration of VSA Host

Before you consider the first power on and primary configuration – you might want to consider your options for creating your second VSA. Although it doesn't take long adding in the VSA, we currently have a VSA which is in a clean and un-configured state. To rapidly create a second VSA – you could run a VirtualCenter "clone" operation to duplicate the current VSA VM configuration. You can do this is even if the VM is located on local storage as is the case with my VSA1.

Lefthand Networks do not support cloning the VSA once it is in a management group setup with the client console used to manage the system.

The primary configuration contains setting the hostname and IP settings for the VSA from a console utility. You can navigate this utility by a combination of keystrokes such as the cursor keys, tab key, spacebar and enter/return keys. It is very simple to use.

1. **Power on both VSA VMs**
2. Open a VMware **Remote Console**
3. **At the Login prompt** – type **start** and press **[Enter]**

```

Welcome to SanIQ

Loading vmlinuz.....
Loading initrd.gz.....
.....
Ready.
Uncompressing Linux... Ok, booting the kernel.
Loading keymap: us [ OK ]

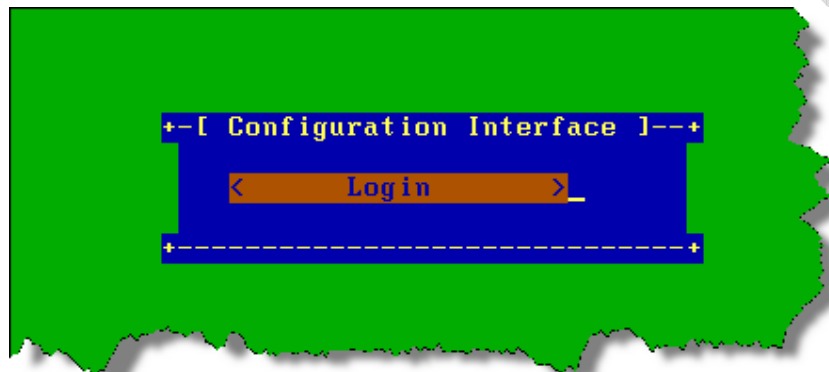
Type in "start" and hit enter at the login prompt.
none login: start_

```

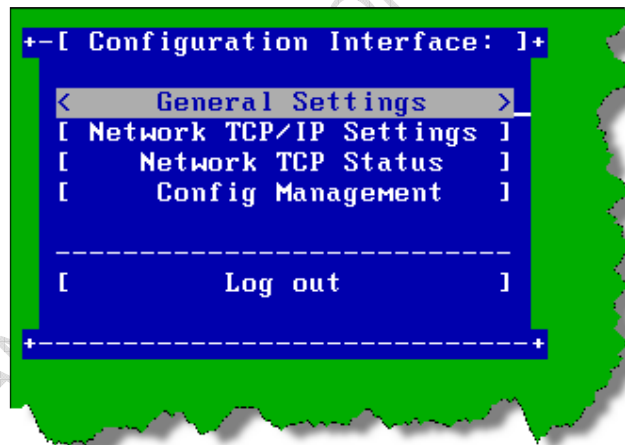
Note:

Images have been inverted here to ease printing. The VSA presents a black background/white text environment

- 4. Press **[Enter]** at the **Login** prompt



- 5. In the menu select **"Network TCP/IP Settings"** and press **[Enter]**



- 6. **Cursor up**, and **select < eth0 >** and press **[Enter]**

```
+--[ Configuration Interface: ]+
[      General Settings      ]
[ Network TCP/IP Settings ]
[ +--[ Available Network Devices: ]+
[
[      < eth0 >_
-----
[      -----
[      [      Back      ]
+-----
+-----
```

7. Change the Hostname and Set a static IP address

```
+--[ Configuration Interface: ]+
[      General Settings      ]
[ Network TCP/IP Settings ]
[ +--[ Avail+--[ Network Settings: ]-----+
[
[      < eth0 > Specify the network settings for the unknown port. Be
-----          sure the ethernet cable is plugged into the selected
[      -----          port.
[
[      -----          Hostname:   vsa1.rtfm-ed.co.uk
+-----
+-----          ( ) Disable Interface.
+-----          ( ) Obtain IP address automatically using DHCP.
+-----          (*) Use the following IP address:
+-----
+-----          IP Address:  172.168.3.99
+-----          Mask:        255.255.255.0_
+-----          Gateway:
+-----
+-----          [ OK ] [ CANCEL ]
+-----
```

8. Press **[Enter]** to confirm the warning about the restart of networking
9. Use the Back options to return to main green/blue login page

Note:

Repeat this process for other VSA, in my case I used the IP address of 172.168.3.98 for the second VSA

TIP:

You might wish to update your DNS configuration to reflect these hostnames and IP address so you can use an FQDN in various management tools

Install Management Client

Advanced configuration is done via LeftHand Networks Centralized Management Console. This is a simple 32-bit application used to remote control and configure the VSA – there is also a Linux version as well. Your management station must have a valid or routable IP address to communicate to the two VSAs. You will find the LeftHand Networks Centralized Management Console free to download from the LeftHand Networks download page

http://www.lefthandnetworks.com/products/saniq_demo.php

I will be using the Windows version CMC Windows (.exe)

The install of the Management Console is very simple, and isn't worth documenting here and a typical installation should be sufficient for the purposes of this guide.

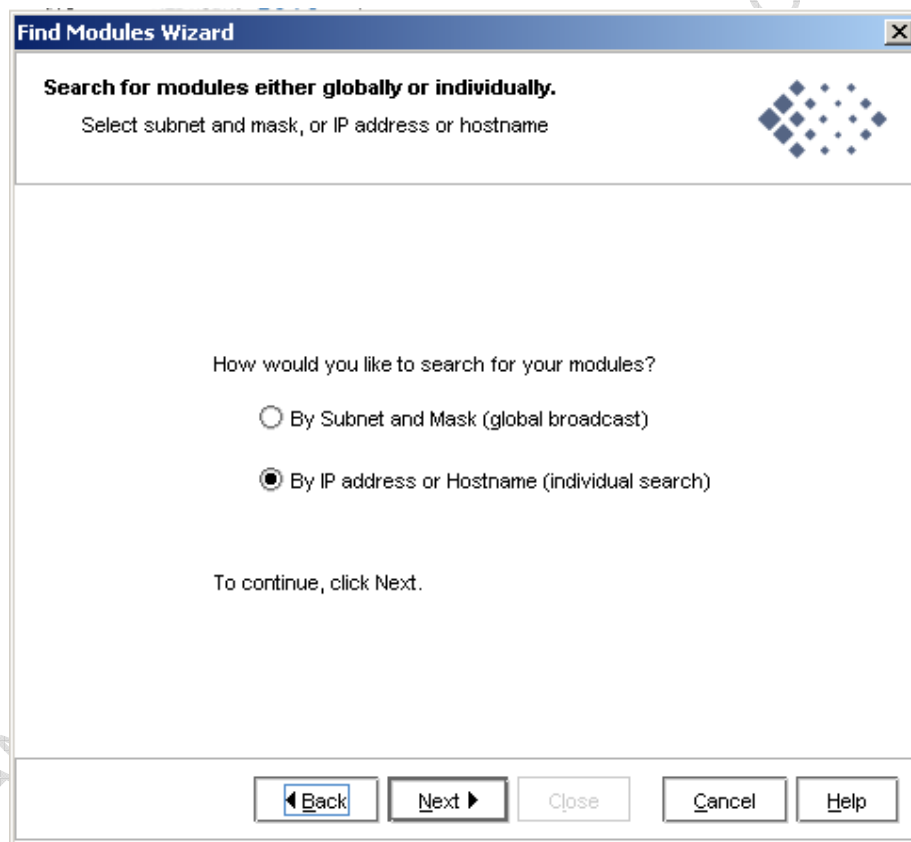
Configure the VSA (Management Groups, Clusters & Volumes)

Adding the VSA's into the Management Console

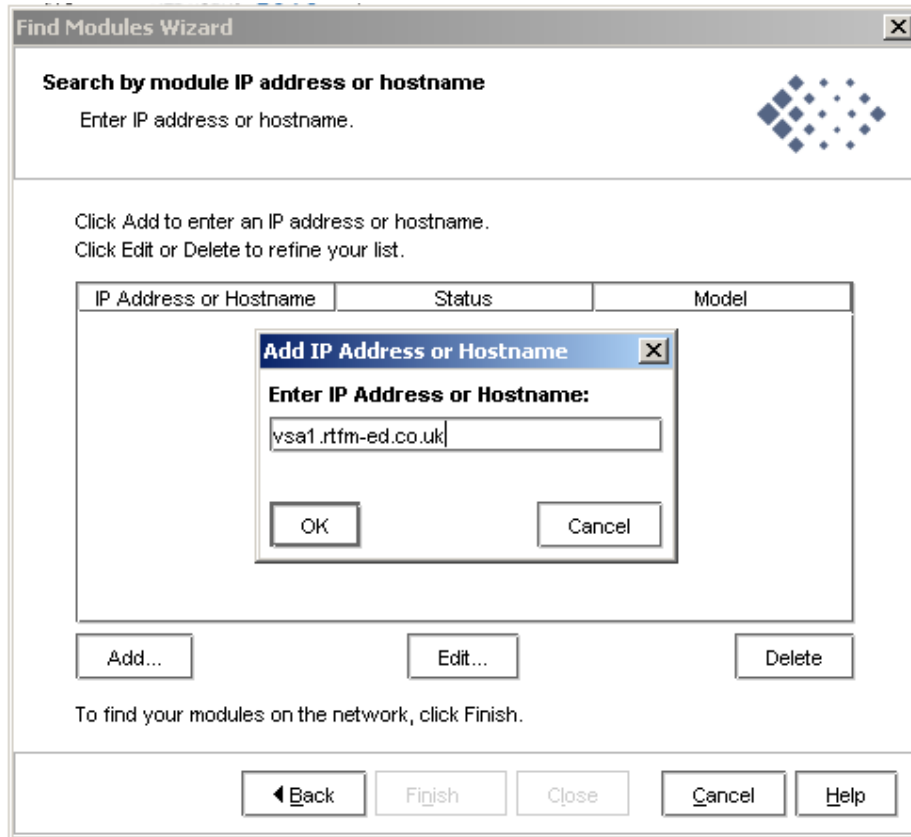
Note:

Before you begin you might as well test you management station can actually ping the VSAs. You're not going to get very far in the next step if you can't.

1. **Load the CMC**, and the **Welcome to Find Modules Wizard** will start
2. Choose to search **By IP Address or Hostname**



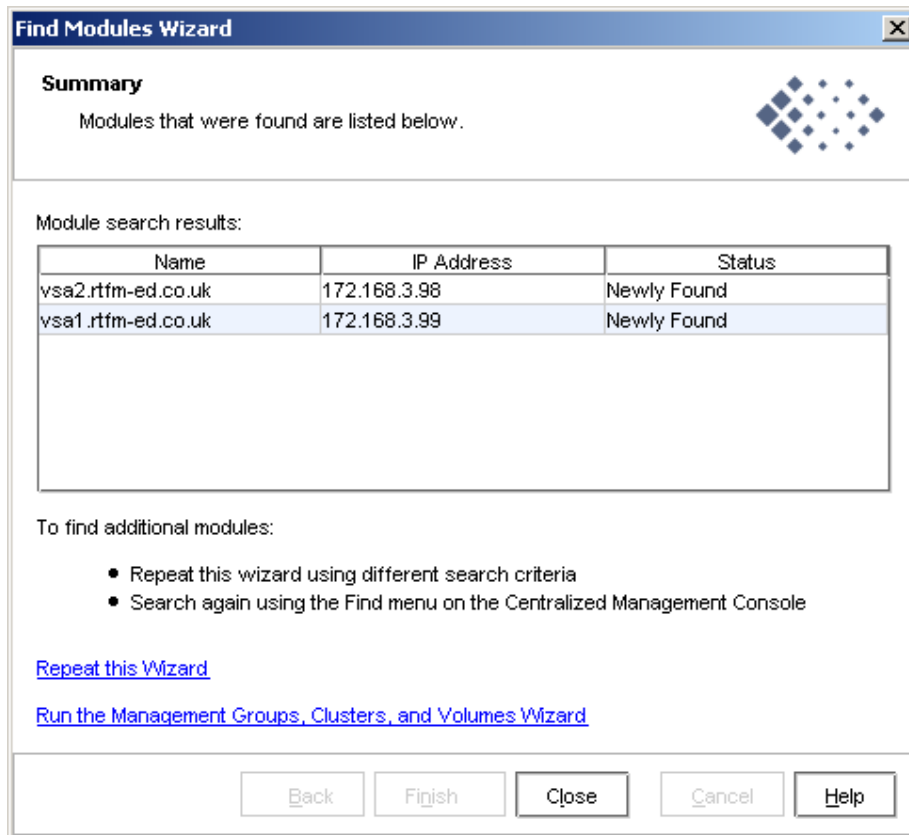
3. Click the **Add** button and **type in the IP Address or Hostname of the VSAs**



Note:

This background dialog may report status as "unknown" until you click Finish, when it will change to "Newly Found"

4. Click **Finish**



5. Click **Close**

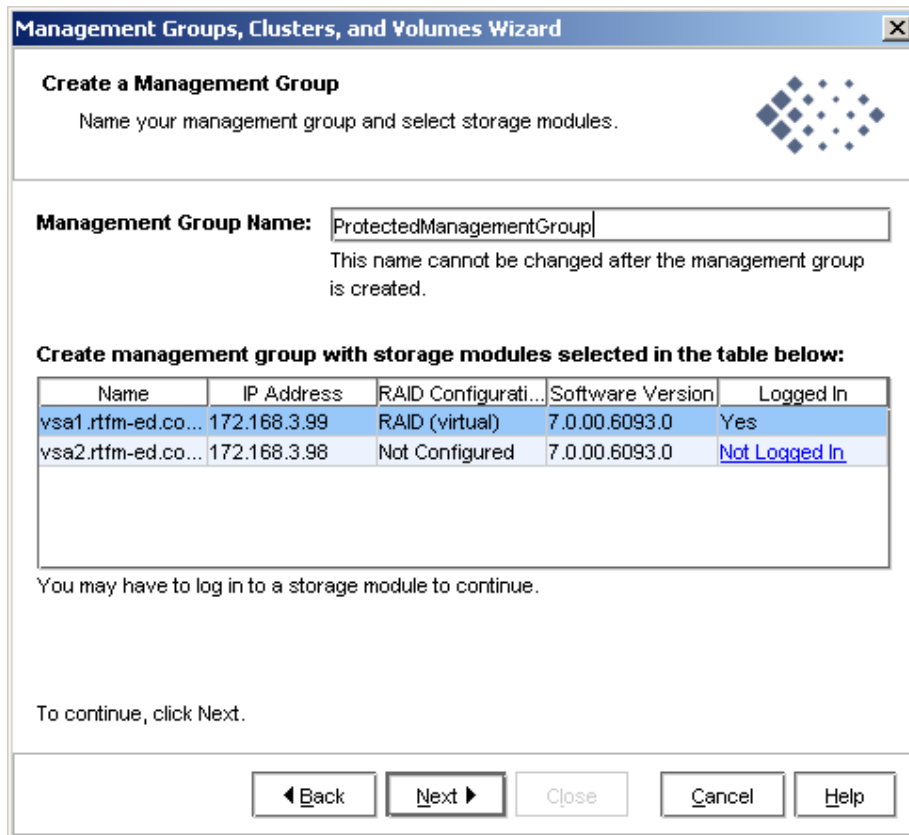
Adding the VSAs to Management Groups

Each VSA will be in its own management group. During this process you will be able to set friendly names for the groups and volume names. It makes sense to clearly use names that reflected the purpose of the unit in question such as:

- ProtectedManagementGroup and RecoveryManagementGroup
- Protected_Cluster and Recovery_Cluster
- Virtual_Machines Volume
- Replica_Of_Virtual_Machines Volume

Of course it is entirely up to you what naming process you adopt. But these names are not allowed to contain a space as a character

1. In the **Getting Started Node**, click **2. Management Groups, Clusters and Volumes** and Click **Next** to Welcome page
2. Choose **New Management Group**
3. For the management group name type something meaningful like **ProtectedManagementGroup** and **Select the VSA you wish to add**, in my case **vsa1.rtfm-ed.co.uk**



Note:

In a production set-up theoretically you could 5 VSA which replicate to each other synchronously in the Protected location, and another 5 VSA's in Recovery location that replicate to each other and with the Protection location in a asynchronous manner.

Spaces are NOT allowed in the Management Group Name. You can use CamelCase or the under_score character to improve readability.

4. Next set a **username** and **password**.

Management Groups, Clusters, and Volumes Wizard

Add administrative user
Add new user information.

User Name: administrator
3-40 characters. Must begin with a letter.

Description: Local administrator account
0-40 characters. Must begin with a letter.

Password: *****
5-40 characters, no "/" or ":" allowed.

Confirm Password: *****

Administrative Group: full_administrator

◀ Back Next ▶ Close Cancel Help

Note:

This username and password is stored in a separate database internally to the VSA. The DB is in a proprietary binary format and is copied to all VSAs in the same management group. If you are the forgetful kinda guy you might want to make some record of these values. It is in no way connected to the logins to your VirtualCenter or Active Directory environment

5. Choose **Manually set time**

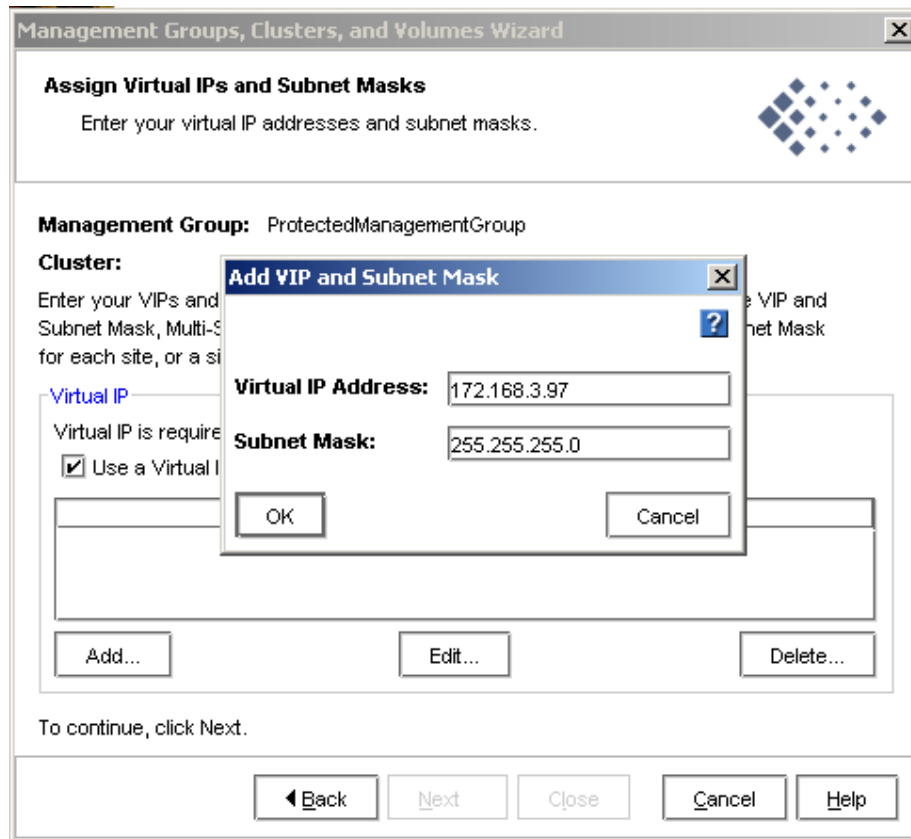
Note:

As the VSA is a virtual appliance it should receive time updates from the ESX host, which is in turn configured for NTP

Create a Cluster

The next stage of the wizard is to create a cluster. In our case we will have one VSA in one management group within one cluster – and separate VSA in different management group within a cluster. The cluster is intended for multiple VSA within one management group, however we cannot setup replication or snapshots between two VSA in different sites without one

1. Choose **Standard Cluster**
2. **Type in a cluster name** such as **Protected_Cluster**
3. **Next set a virtual IP**, this is mainly used by cluster within a management group and strictly speaking isn't required – but it's a good idea to set this now for possible future use. In my case I used the next available IP of 172.168.3.97



Create a Volume

The next step is creating a volume. Volume is another word for a LUN. Whatever word you are familiar with we are creating a block of storage which is unformatted which could be address by another system (in our case ESX) once formatted files could be created on it.

A volume can either be full or thinly provisioned. With thinly provisioned volumes the on-disk space can be less than the volumes size. You might know this is as virtual storage where you procure disk space as you need it rather than up front. The downside is you must really track and trace your actual storage utilization very carefully. You cannot save files in thin air.

1. **Type in a volume name** such as: **virtualmachines**
2. **Set the volume size** such as: **1TB**
3. Choose **Thin** for Provisioning

Management Groups, Clusters, and Volumes Wizard [X]

Create Volume
Name your volume and choose a size appropriate for its intended use.

Type: Primary

Volume Name: virtualmachines
This name cannot be changed after the volume is created.

Description: Used to store VMs

Replication Level: None

Max Size: 48.062 GB (if fully provisioned)

Size: 1 TB

Provisioning: Full Thin

To create the volume, click Finish. Skip Volume Creation

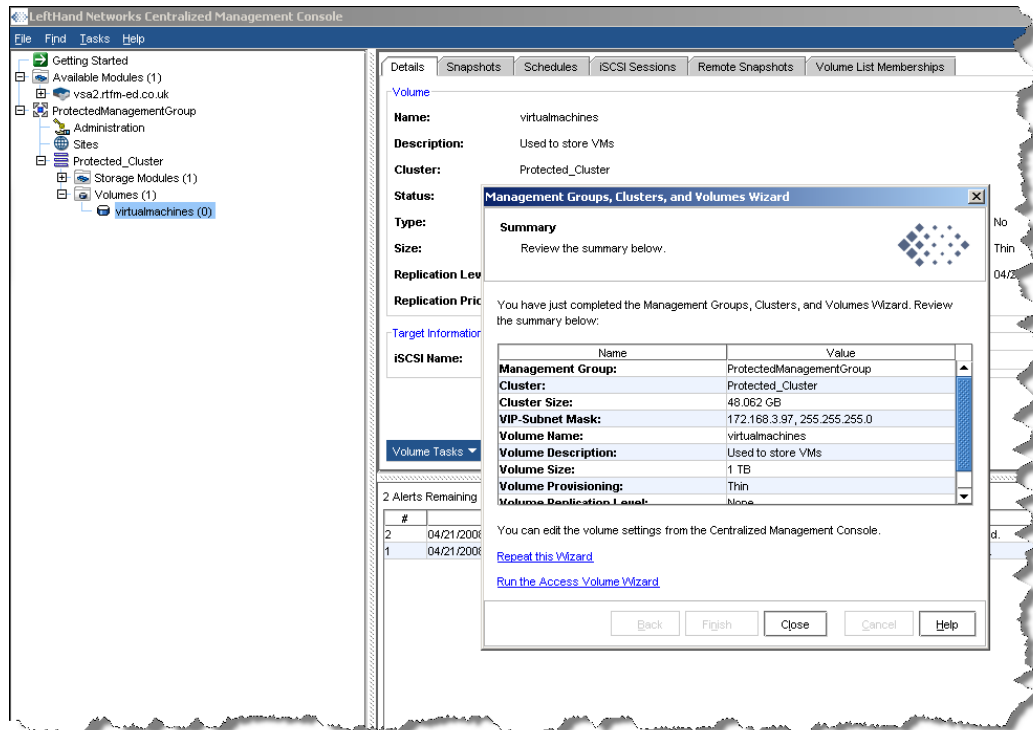
◀ Back Finish ▶ Close Cancel Help

Note:

In this case I create a volume called virtualmachines which is used to store VMs. The size of the "physical" disk is 48GB, but with thin-provisioning I am going to present this storage as if it was 1TB volume/LUN. Replication level would be used if I was replicating *within* a management group. In the case of this configuration it is irrelevant because we are replicating *between* management groups.

You can switch to/from Thin to Full at any time you wish.

At the end some quite lengthy status bars the management group, cluster and volume will have been created



Note:

Now repeat this process for VSA2 but using unique names and IP address

Management Group Name: RecoveryManagementGroup
Cluster Name: Recovery_Cluster
Volume Name: replica_of_virtualmachines

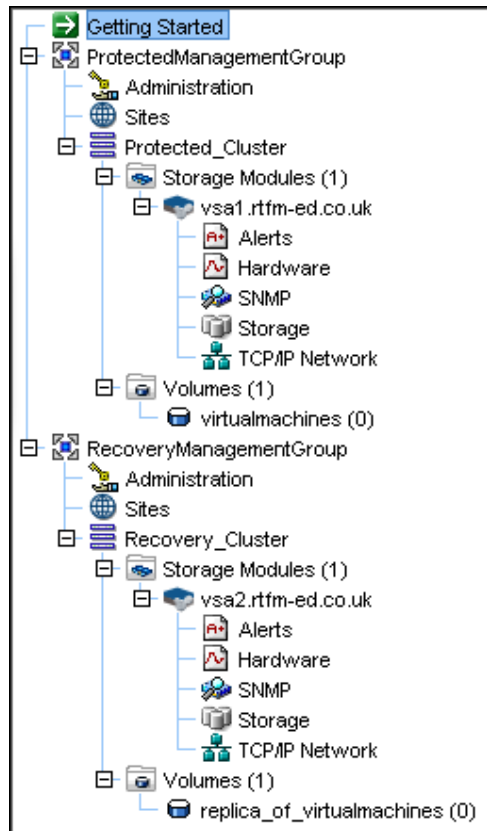
Note:

Different vendors use different terms for copying a piece of data to another such a remote copy, replication and snapshot. All of these terms in the world of storage mean much the same thing. A duplication of data from one location. I've always called this replication hence the use of term replica_of_virtualmachines. You might have notice I have used the phrase replication or snapshot throughout this guide because me the two much the same concept.

Note:

At the end of this process you should have view which looks similar to this:

SAMPLE - NOT FOR REUSE!

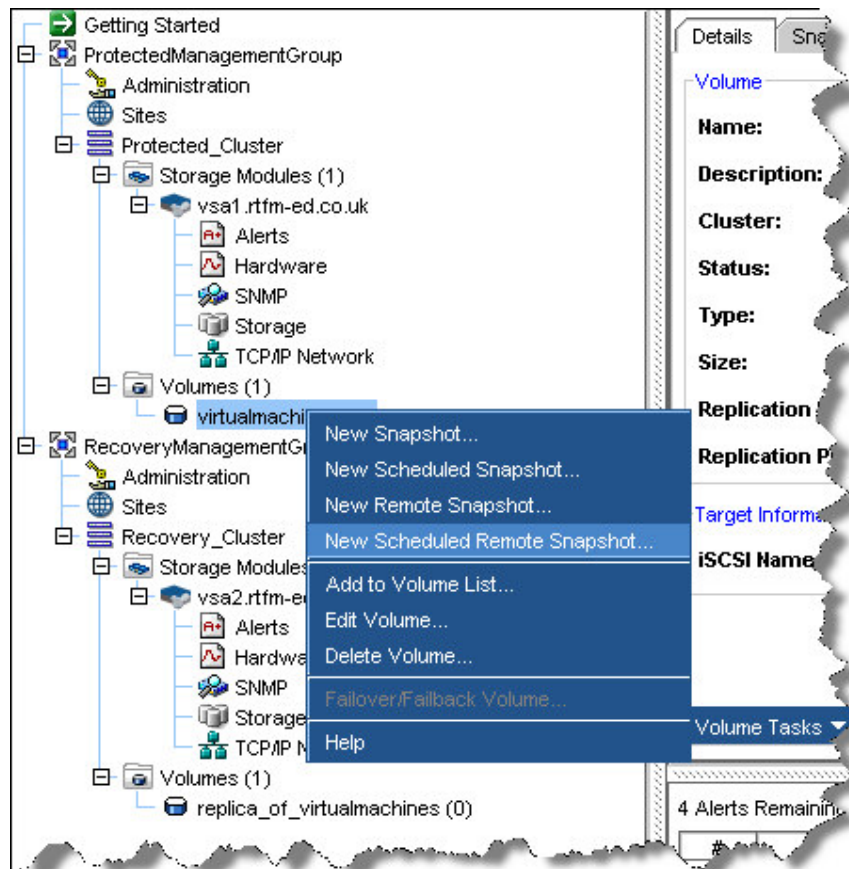


Configuring VSA for Replication

It is very easy to setup replication or a snapshot between two VSA's in two different management groups. The best option to go for in terms of SRA is a "Schedule Remote Snapshot". This allows for asynchronous replication between two VSA at interval of your choosing.

In the VSA the protect volumes a snapshot is taken at the protected location, once completed this snapshot is then replicated to the recovery location. After the first copy the only data transferred are the changes – or deltas. We have setting to control the retention of this data. The snapshot process can be as frequent as every two minutes and we can control how long to retain the snapshot data both at the Protected and Recovery management groups

1. In **the ProtectedManagementGroup, Protected Cluster, Volumes**
2. **Right-click your volume** and choose **New Schedule Remote Snapshot**



3. Set the Recur Every to be every 30 minutes

4. Under "**Primary Snapshot Setup**" enable the option to be **Retained for a maximum** of **3** snapshots.

Note:

Its really up to you how long you keep your snapshots. In this configuration I would have 3 snapshot in 180 minutes, when the fourth snapshot was taken the oldest one would be disregarded. Obviously, the longer you retain your snapshot the more options exist for data recovery. In this test environment we configuring you probably won't want to hang on this data for too long. The more frequently you take snapshots and the longer you retain them the more storage space you will require. For testing purposes you might find a much less frequent intervals will be appropriate – as you need less space to retain the snapshots

5. Under "**Remote Snapshot Setup**", select the **RecoveryManagementGroup** and
6. Under **Volume name**, ensure you have your **replica_of_virtualmachines** selected
7. Click **Retain maximum of:** and set the value to be **3** snapshots

Name: virtualmachines_RS_Sch_1

Description:

Start At: Select 'Start At' time -> Edit...

Recur Every: 30 Minutes

Next Occurrence: N/A

Primary Snapshot Setup

Management Group: ProtectedManagementGroup

Volume Name: virtualmachines

Retain Snapshots For: 1 Weeks

Retain Maximum Of: 3 Snapshots

Remote Snapshot Setup

Management Group: RecoveryManagement...

Volume Name: replica_of_virtualmac... New Volume...

Retain Snapshots For: 1 Weeks

Retain Maximum Of: 3 Snapshots

OK Cancel

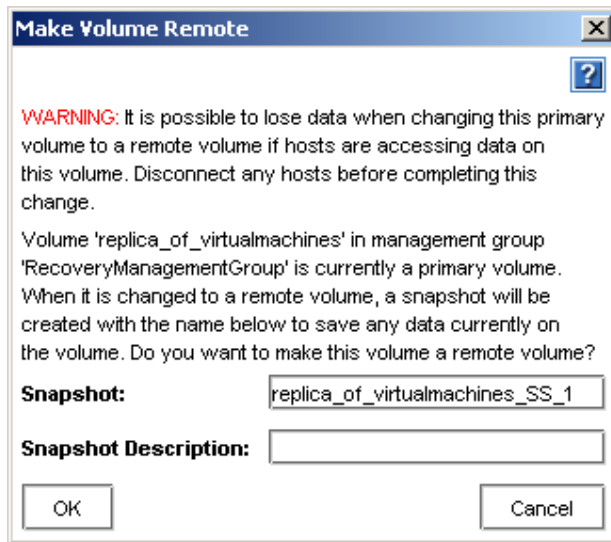
Important:

You will notice that despite setting all these parameters the OK button has not been enabled. This is because we have yet to set start date or time for the first snapshot

Caution:

The frequency of the snapshot and retention values are important. If you create a two shallow a replication cycle as I have done here you could be mid-way through a test of your recovery plan only to find the snapshot you were currently working on is purged from the system. In the end because of lack of storage I adjust my frequency to be an hour – as about midway through writing this book I ran out of storage, and that was with system that wasn't generating much in the way in new files or deleting old files

8. Next to **Select 'Start At' time**, click **Edit** button – and using the date and time interface when you would like the replication/snapshot process to begin.
9. Click **OK**
10. Click **OK** to the **"Make Volume Remote"** warning dialog box



Note:

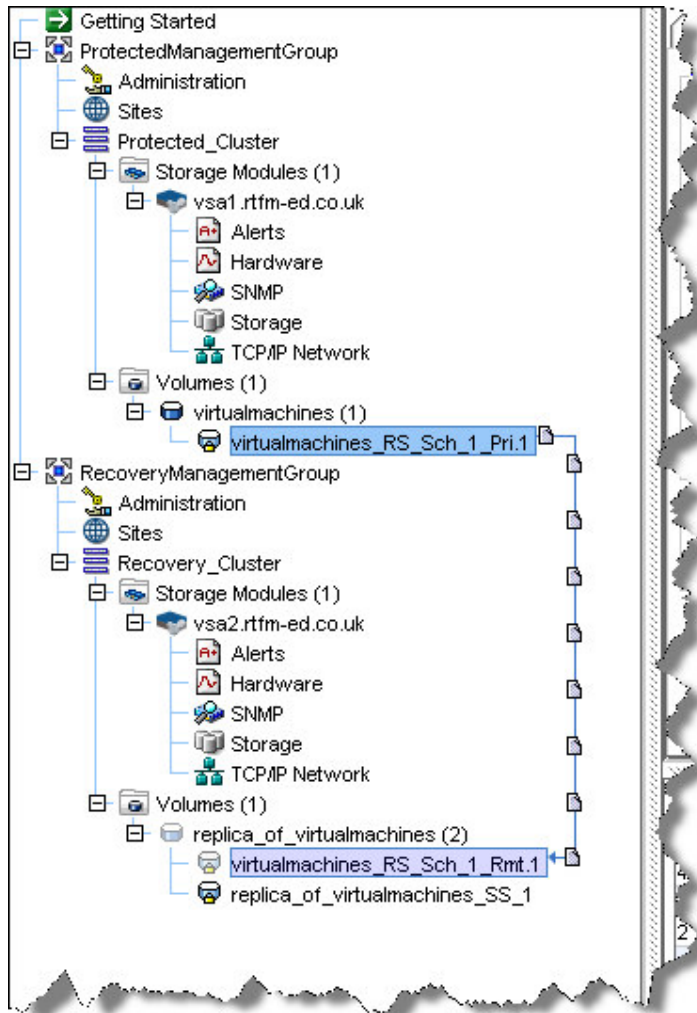
This dialog box is just concerned that destination volume (here called replica_of_virtualmachines) may already contain data. The replication/snapshot process will over-write this volume. To prevent data lost the VSA snapshots this volume also.

Note:

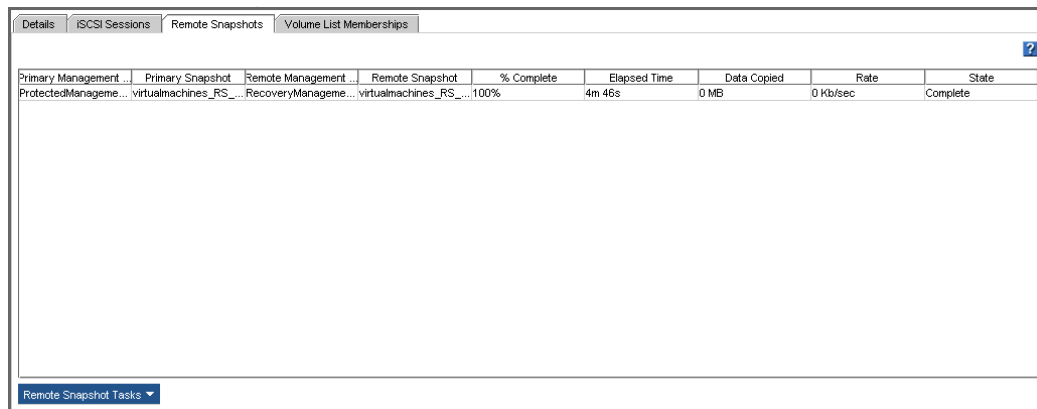
If you have not licensed the VSA this feature will work but only for another 30-days. You may receive warnings about this if you are working with an evaluation version of the VSA.

Monitoring your replication/snapshot

Of course, you will be wondering if it's working. There a couple ways of to tell. Expanding the volumes within each Management Group, this will expose the snapshots. You might see the actual replication in process with animated icons like in the screen grab below



After selecting the remote snapshot, you will see a tab on the right-hand side labelled "Remote Snapshots". This will tell you how much data was transferred and how long it took complete.



Creating Volume Lists and Authentication Groups

Clearly, there would be little security if you could just give your ESX host an IP address and "point" them at the storage. To allow your ESX hosts access to the storage we must complete three main steps

- **Create volume list**
Literally this is a list of volumes that hosts can access. In our simple configuration this will contain just one volume – but it could contain many volumes
- **Authentication Group**
This contains the host you wish to grant access – in our case an ESX host. Authentication Groups contain a single host, and these "groups" are allowed access to the volumes. As you might expect authentication groups can contain CHAP (Challenge Handshake Authentication Protocol) settings in addition to the IQN value. One thing that feels a little odd about that is how these "groups" only contain one object – a reference to a single ESX host. But this is correct, it just feels a bit odd in the GUI
- **IQN (iSCSI Qualified Name)**
Each ESX host will be allocated a IQN – the IQN is used within the authentication group to identify an ESX host. In case you have forgotten, the IQN is convention rather than an hard-coded unique name (unlike the WWN's found on Fibre-Channel Devices) and take the format of `iqn-date-reverse-fqdn:alias`. As a domain name can only be registered once on a particular date (albeit they can be transferred or sold to another organization) they do impose a level of uniqueness fit for their purpose. An example IQN would be:

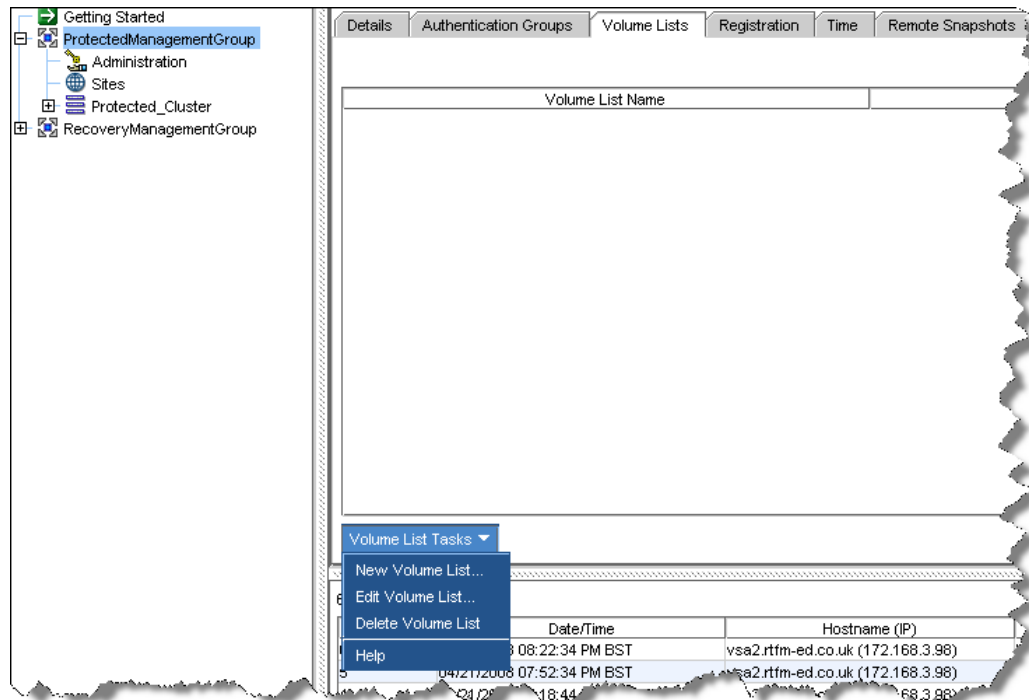
iqn.2001-09.uk.co.rtfm-ed:esx1

In this simple set-up my ESX hosts are in the Protected Site, and they are imaginatively called `esx1.rtfm-ed.co.uk` and `esx2.rtfm-ed.co.uk`. My other two ESX hosts (yes, you guessed it - `esx3` and `esx4`) are the Recovery Site and do **not** need access to the volume in the protected management group. Before I invoke DR/BC with SRM the Site Recovery Agent will have grant them access to the latest snapshot of `replica_of_virtual_machines`. For the moment ESX3 and ESX4 need no access to the VSAs at all.

Creating a Volume List

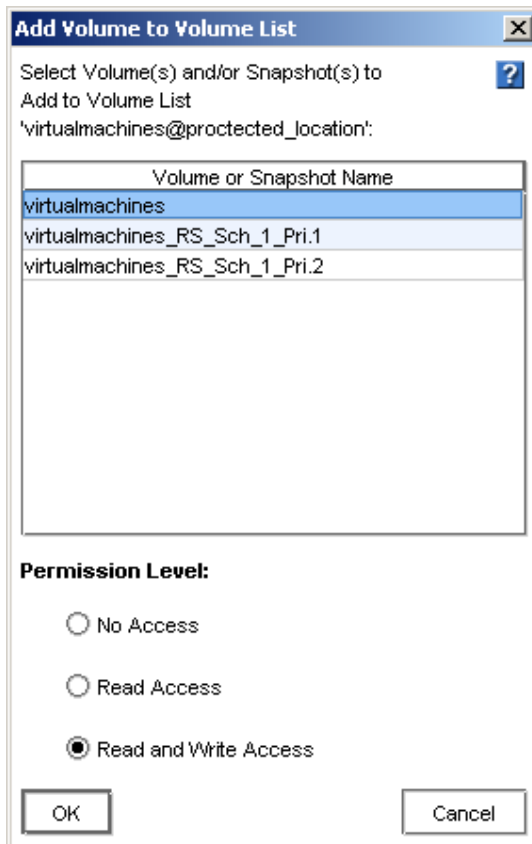
1. The **ProtectedManagementGroup**
2. In the tabs on the right-hand side – choose **Volume List** tab

3. Click the **Volume List Tasks**, and select **New Volume List**

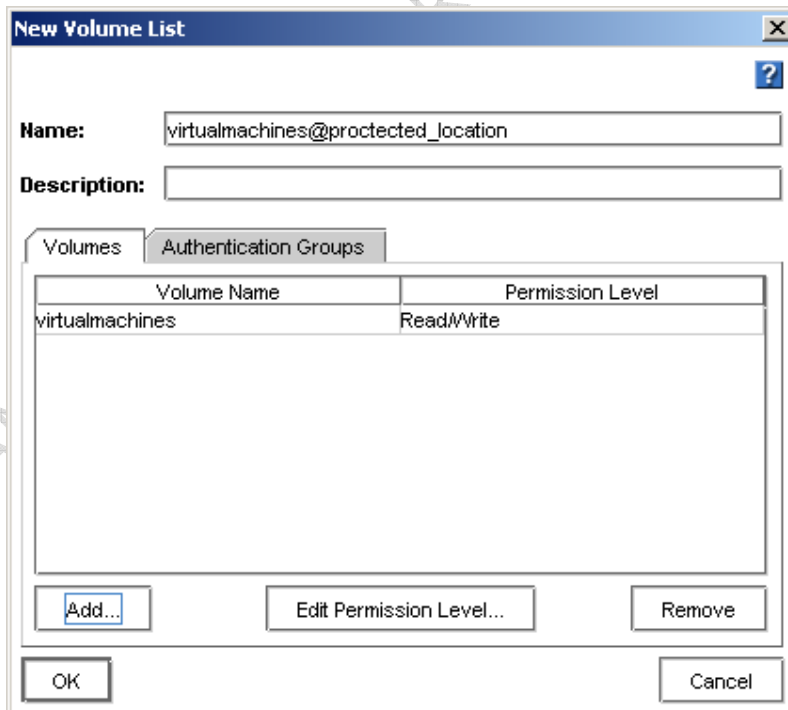


4. **Type in a friendly name for the Volume List** such as virtualmachines@protected_location
5. Then click the **Add** button, and select the **virtualmachines** volume and **ensure the permissions level** is set to **Read/Write Access**

SAMPLE - NOT FOR REUSE



Note: This screen grab above shows me selecting the right-volume



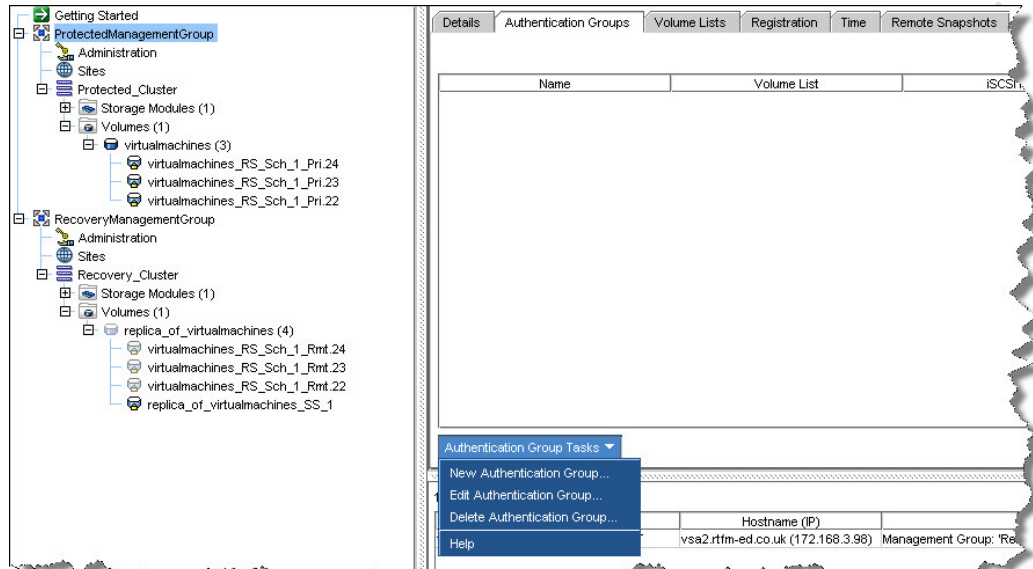
Note: Whereas this dialog box above shows the volume being added to the volume list

6. Click **OK**

Creating Authentication Groups and Setting the IQN

Authentication Groups are objects in Lefthand Networks VSA contain the parameters that allow an ESX host access to the volume list. They must contain a valid IQN value, and optionally CHAP authentication settings.

1. The **ProtectedManagementGroup**
2. In the tabs on the right-hand side – choose **Authentication Groups** tab



3. Click **Authentication Group Tasks**, and **New Authentication Group**
4. **Set a descriptive name for the Authentication Group** such as: **esx1.rtfm-ed.co.uk**
5. **Select from the Volume List** pull-down, the volume list you create previously – in my case **virtualmachines@protected_location**
6. Under "**Authentication**" click into the **Initiator Node Name** edit box, and type your IQN such as **iqn.2001-09.uk.co.rtfm-ed:esx1**

SAMPLE - NOT FOR

Note:
CHAP authentication is not required to make the VSA work with SRM, but does offer an additional layer of security

7. Click **OK**

Note:
Repeat this process for any other hosts in your Protected Site that needs access to the same volume/LUN

Conclusion

For now this completes the configuration of the VSA – all that remains to do is to configure the ESX host connection to the VSA. Currently our ESX hosts in recovery location have no access to VSA, and will not need it until we test or invoke are DR/BC plan.

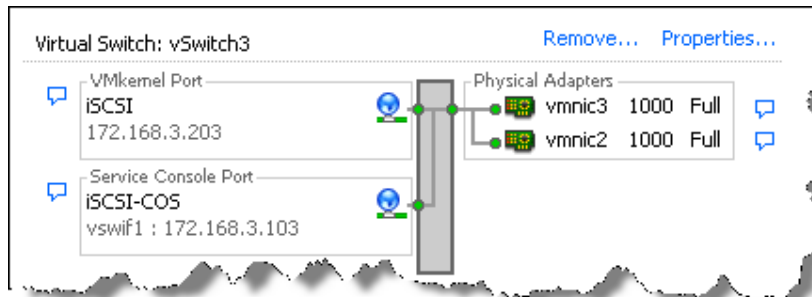
Configuring the ESX Software iSCSI

If you have a dedicated iSCSI hardware adapter you can configure your IP settings and IQN directly on the card. The huge advantage of this is that if you wipe your ESX host, you iSCSI settings remain on the card. In the absence of a supported iSCSI hardware

adapter – you can the ESX hosts own software adapter. The following instructions explain how to set it up to speak to the VSA.

Before you enable the Software Initiator/Adapter in the ESX host you will need to create both a VMkernel and Service Console port with the correct IP data to communicate to the VSA. The reason you need the Service Console port - is whilst the main I/O is driven by the VMkernel and its IP stack, part of the discovery of volumes/LUN (SendTargets) and CHAP Authentication is in the Service Console still. Therefore both the VMkernel and the Service Console kernel need access. This does not apply in the case of ESX3i where only a VMkernel port is needed.

The diagram below shows my configuration for esx1 and esx2, notice the vSwitch has two NICs for fault-tolerance.



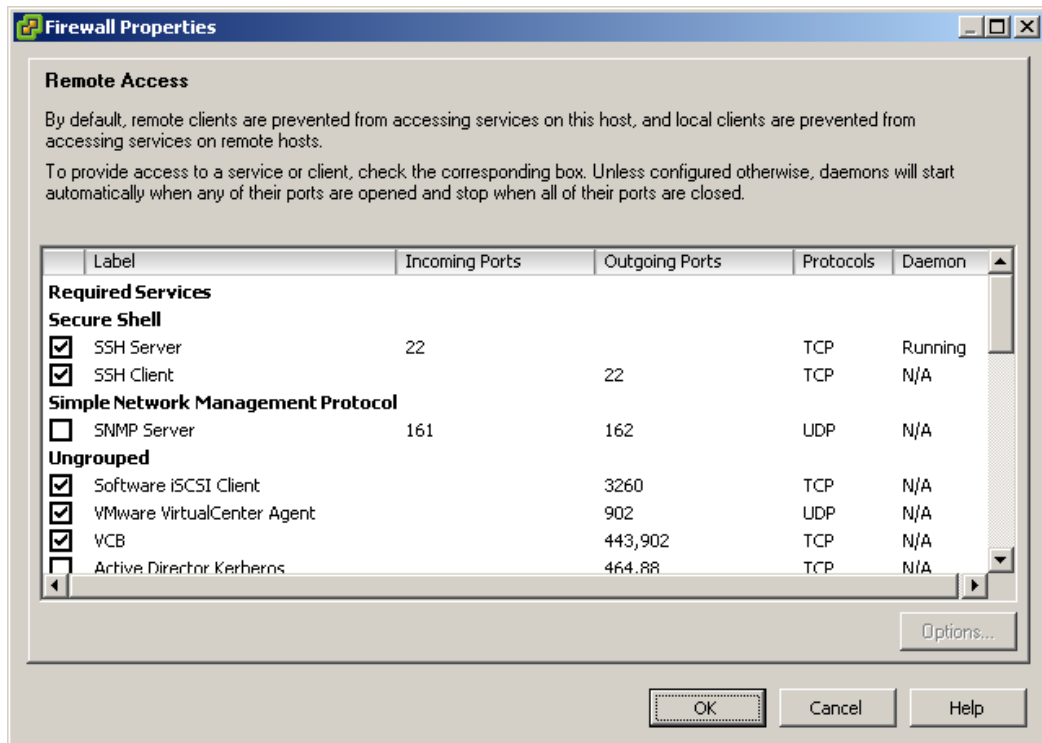
Before proceeding with the configuration of the VMware software initiator/adapter you might wish confirm you can communicate with the VSA by using a simple ping test.

Enabling the iSCSI Initiator

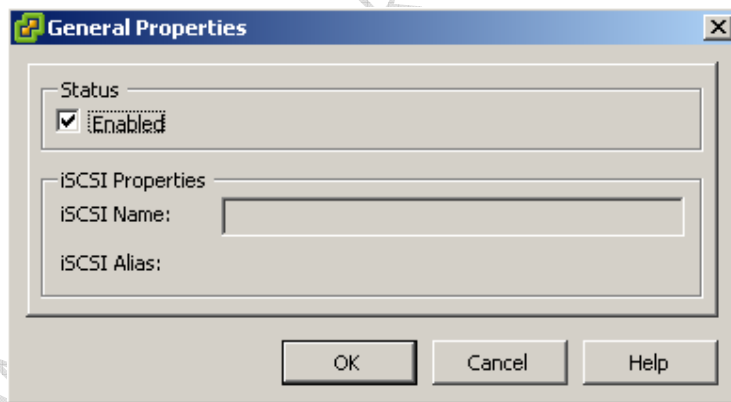
Note:

Depending on the version of ESX you are using – you may or may not need to manual open the iSCSI Software TCP Port on the ESX firewall. I've always done this manually – to be 100% certain there is no communication barrier between the ESX hosts and the iSCSI Target

1. **Select the ESX host**, and the **Configuration** Tab
2. Select the **Security Profile** link, in the **Software Tab**
3. Click the **Properties...** link
4. In the dialog box open the **TCP Port (3260)** for the **iSCSI Software Client**



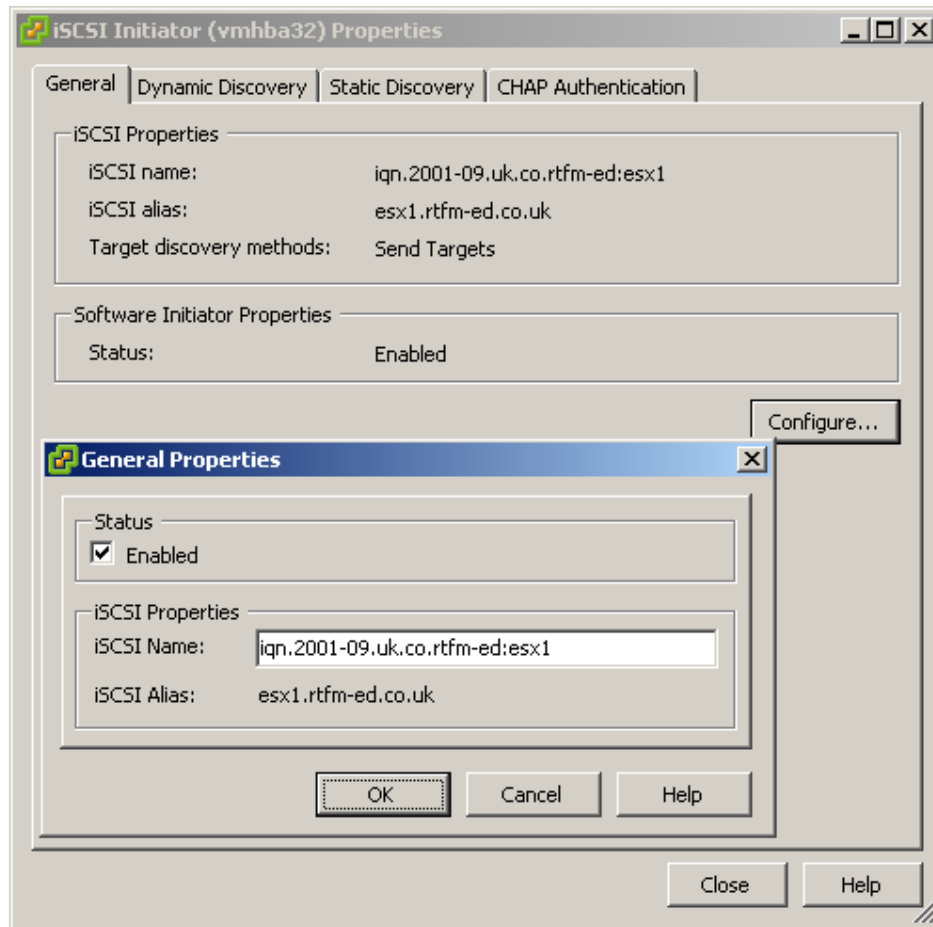
5. Next click the **Storage Adapter** link and select the **iSCSI Software Adapter**
6. Choose **Properties...**
7. In the dialog box click the **Configure** button
8. **Enable the option under status**, as shown below



Note:

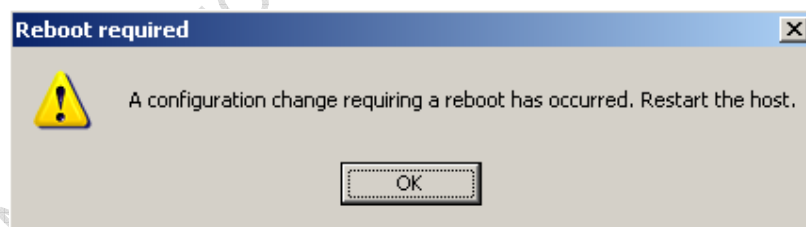
This can take some time. Be patient. You will not be able set a custom IQN until you click OK. VMware will try to help you out by setting a default IQN.

9. Click the **Configure** button again, replace the auto generated IQN with your own standards like so:



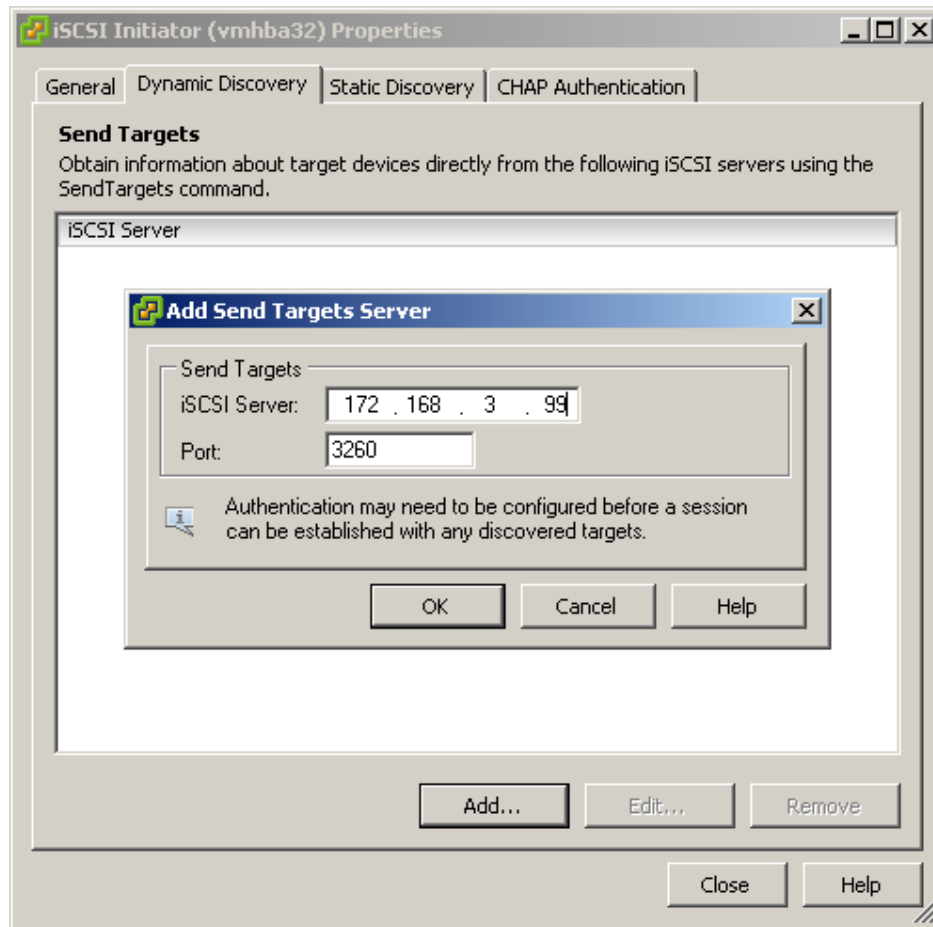
Note:

After clicking OK, this time – a dialog box will appear indicating you must reboot the ESX host



This is true, but we will defer the reboot until we are finished completely

10. Next select the **Dynamic Discovery** Tab, and Click the **Add** button
11. **Type in the IP address of the VSA** in your **Protected_Mangement_Group** in my case, **172.168.3.99**



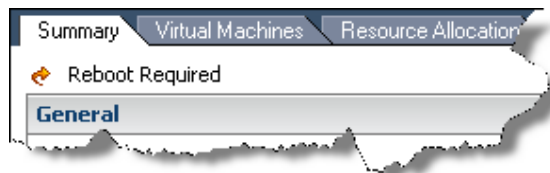
Note:
 Static discovery is only supported with hardware initiators. CHAP Authentication is optional, and I have not configured it in this guide.

12. Click **OK**

Note:
 This can take some time as well

13. Then **reboot the ESX host**

Note:
 If you do not reboot the ESX host, when a warning will be on the Summary Tab of the ESX host



Monitoring your iSCSI Connections

There are many places where you can confirm you have a valid iSCSI connection. This is important because networks can and do fail.

In the first instance you should be able to see the volume/LUN in the Vi client:

Details

vmhba32 [Properties...](#)

Model:	iSCSI Software Adapter	IP Address:	
iSCSI Name:	iqn.2001-09.uk.co.rtfm-ed:esx1	Discovery Methods:	Send Targets
iSCSI Alias:	esx1.rtfm-ed.co.uk	Targets:	1

SCSI Target 1

iSCSI Name:	iqn.2003-10.com.lefthandnetworks:protectedmanagementgroup:11:virtualmachines
iSCSI Alias:	
Target LUNs:	1 Hide LUNs

Path	Canonical Path	Type	Capacity	LUN ID
vmhba32:1:0	vmhba32:1:0	disk	1.00 TB	0

Note: On the properties of the "virtual" hba, in this case vmhba32

vmhba32:1:0 Manage Paths

Policy

Fixed
Use the preferred path when available [Change...](#)

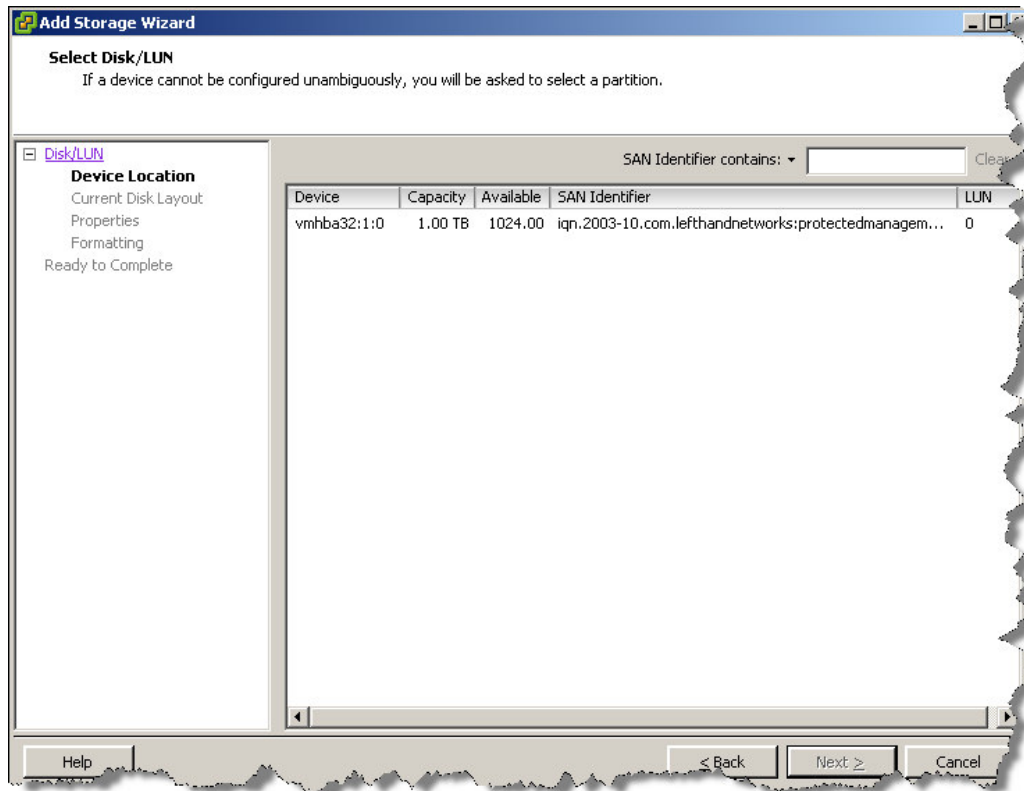
Paths

Device	SAN Identifier	Status	Preferred
vmhba32:1:0	iqn.2003-10.com.lefthandne...	Active	*

[Refresh](#) [Change...](#)

[OK](#) [Cancel](#) [Help](#)

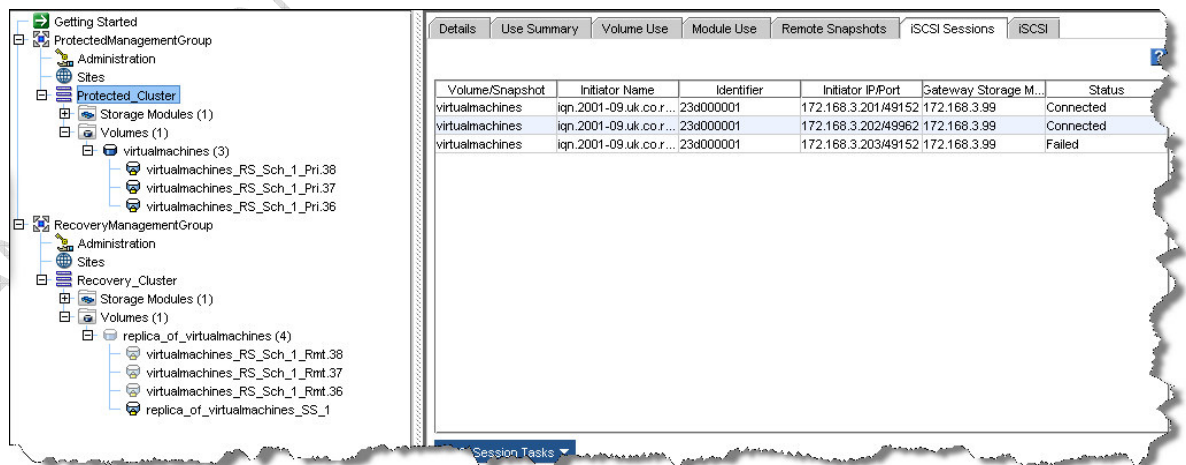
Note: By right-clicking the volume/LUN and seeing the status in green and set to active



Note: When you add storage you should see the volume/LUN

However, more specifically you can see the status of you iSCSI connections from the VSA's management console

1. Expand the **Protected_Mangement_Group**
2. Select the **Protect_Cluster**, and click the **iSCSI Sessions Tab**



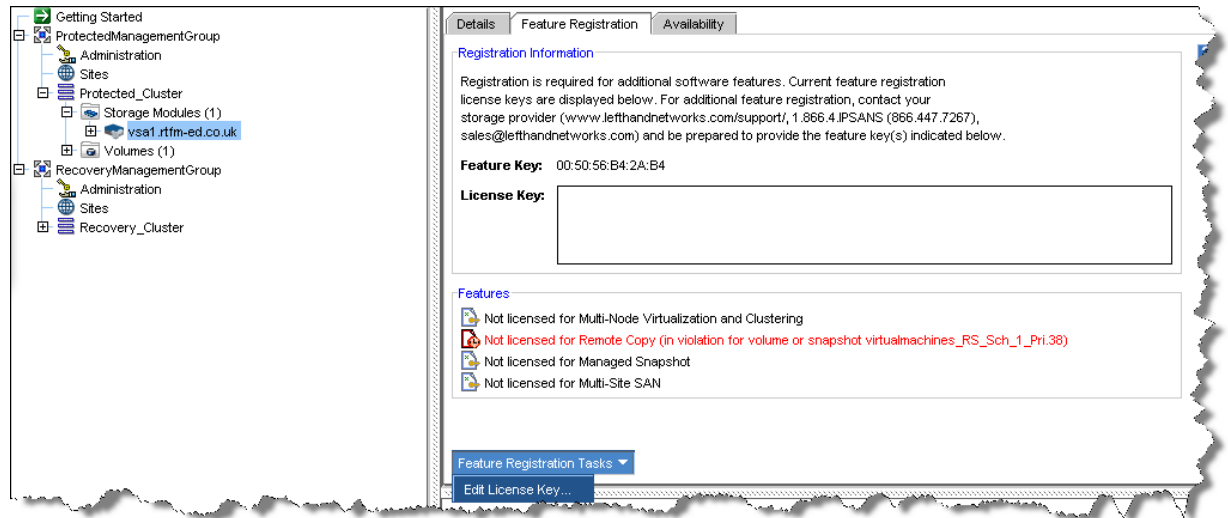
Note:

In this case you can see there was 3 session but one of them failed. This was caused by removing the iSCSI settings on ESX3 whilst it was connected to the VSA

Licensing VSA

Should you go ahead and purchase the VSAs they are licensed per VSA. As mentioned previously the license is attached to the MAC address of the VSA. Once you have registered your MAC with Lefthand Networks you will be issued with appropriate license strings. To input your license strings the following procedure is needed

1. **Expand + ProtectedManagementGroup, + Protect_Cluster, + Modules**
2. **Select your VSA, and click the Feature Registration Tab**



Notice:

The UI shows the MAC address of the VSA above the license key field

3. Select the **Feature Registration Task** and Select **Edit License Key**
4. Then use cut and paste to add your license key

Shutting Down the VSA

It is recommended to use the VSA Management Console to take a VSA offline.

1. **Right-click** the **Management Group**
2. Choose **Shutdown Management Group**

Conclusion

In this section I have quickly shown you how to setup a 30-day evaluation copy of virtual appliance which is suitable for use with VMware SRM. We setup two Lefthand Networks VSA's and then configured them for replication/snapshot. Lastly, we connected an ESX host to that storage.

From this point onwards you could format the volume/LUN with VMFS and create virtual machines. You might wish to do that – so you have some test VMs to use with VMware SRM. When you do create your VMs use VMware's virtual disks. At the moment VMware's RDM feature is only experimentally supported with SRM. Despite this "experimental support" I will be covering RDMs latter in this book – because it is an extremely popular VMware feature.

In the next chapter will be installed Site Recovery Manager.