SteelCentral™ AppResponse 11 Virtual Edition Installation Guide

Virtual Edition for VMware ESXi 5.5 and ESXi 6.0

Version 11.4.x

March 2018

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com

712-00308-08

Contents

About this guide

The Riverbed® SteelCentral™ AppResponse 11 virtual edition is a virtualized implementation of the SteelCentral AppResponse 11. It provides visibility into virtual environments by monitoring all applications and traffic traversing the hypervisor.

If you are acquainted with the physical AppResponse 11, you will find the AppResponse 11 virtual edition similar in structure and function.

This guide details the steps to deploy AppResponse 11 on a VMware ESXi host.

Upgrading a VMon or v2000 Virtual Appliance to AppResponse 11.4 or Later

AppResponse 11.4 or later can be installed on an existing AppResponse VMon or v2000 virtual appliance. Before you upgrade, please review "AppResponse Release 11.4.0: Compatibility, Feature, and Upgrade Process Overview" for more information. AppResponse Xpert 9 version 9.6.2 provides a feature that creates an off-line archive for existing content. Customers requiring retention of their AR9 disk-based content are advised to postpone their upgrade until this new feature becomes available with the release of AR9 9.6.2.

Note: For a successful upgrade, all storage must be healthy. Correct any storage issues before this installation.

Important: The existing AppResponse 9 software is overwritten and all data is deleted.

There is no means to recover AppResponse 9 or any of its data after AppResponse 11 is installed.

If you are running ARX 9.6.x, you can access the AppResponse 9 performance data if you create an archive of the AppResponse 9 installation *before* you upgrade to AppResponse 11. Please see the *SteelCentral AppResponse 9.6.2 Release Notes* for more information.

Riverbed recommends the following:

1. Create an archive of the performance data on the AppResponse 9 appliance. For details, see the *SteelCentral AppResponse 9.6.2 Release Notes*.
2. Export the Business Groups and Application definitions from AppResponse 9; you can import these definitions into AppResponse 11 after the upgrade. For details, see the *SteelCentral AppResponse 9.6.2 Release Notes*.
3. Note the network settings for the management interfaces on the appliance. See "Setting up the initial configuration" for the network information that you will need to configure AppResponse 11 after the upgrade.
4. Transfer custom WTA configuration. For details, see the *SteelCentral AppResponse 9.6.2 Release Notes*.
5. Configure AppResponse 11. For details, see the "Configuring AppResponse 11 Virtual Edition" section of this document.

Preparing to deploy AppResponse 11 Virtual Edition

System Requirements

Make sure you have these system components available or installed, as appropriate.

- VMware ESXi 5.5 or 6.0 running on a server.
  Important: the host CPUs *must* support the POPCNT CPU instructions (the Nehalem generation of Xeon CPUs (or later).
  The server needs to have:
  - a virtual machine with 4 virtual CPUs
  - 8 GB of RAM

  Packet Storage, depending on your model
  - No packet storage

    - up to 100GB (100v and Flow)
    - up to 2TB (500v)
    - up to 8TB (2000v)
- Web browser - Tested using Internet Explorer 11, Chrome 51 and Firefox ESR 45. Other versions or browsers may not be compatible.

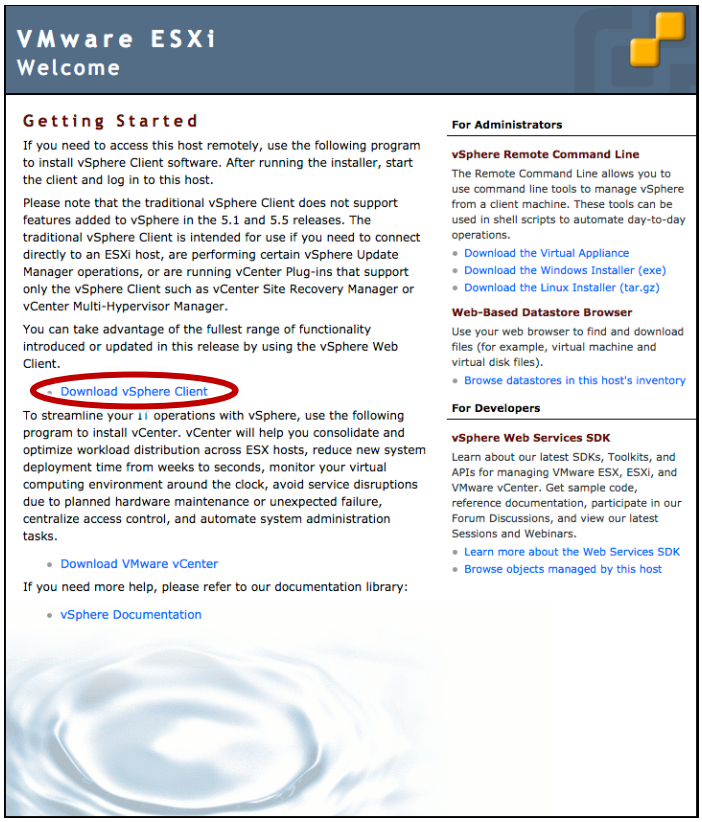
Gathering the software components

Make sure you have these software components available or installed, as appropriate.

- AppResponse 11 OVA package, stored on your local system
- VMware vSphere Client, installed on your local system

If you do not have the vSphere Client on your local system, you can download it from the ESXi host, as follows:

1. Point your web browser at the ESXi host. You should see this welcome page:



2. Click the **`Download vSphere Client`** link on the welcome page and save the installation file to your local system. Note that the vSphere Client is Windows-only software.
3. Run the vSphere Client installation file and follow the instructions on the screen.

Access to network

If you lock down your network on a port-by-port basis, ensure that the following ports are open between the AppResponse 11 and other devices it must communicate with:

- **TCP/22** – (ssh) Command line interface
- **TCP/443** – (https) Web interface and control from Riverbed® SteelCentral Packet Analyzer.
- **UDP/123** – (ntp) Time synchronization

Preparing the ESXi server

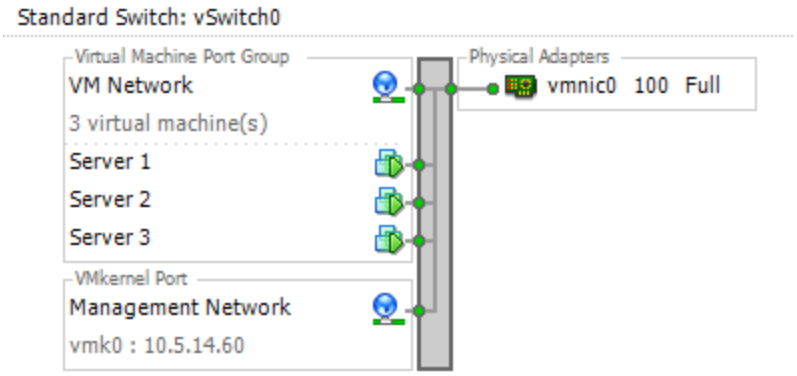
The AppResponse 11 software you deploy to the server comes in the form of an AppResponse 11 OVA package. This package is preconfigured with these virtual components:

- `primary` primary management port
- `aux` secondary management port
- `mon0` primary monitor (data capture) port
- OS disk operating system disk for the AppResponse 11 (100GB)

After you have deployed the OVA package to the server, you can add more virtual components:

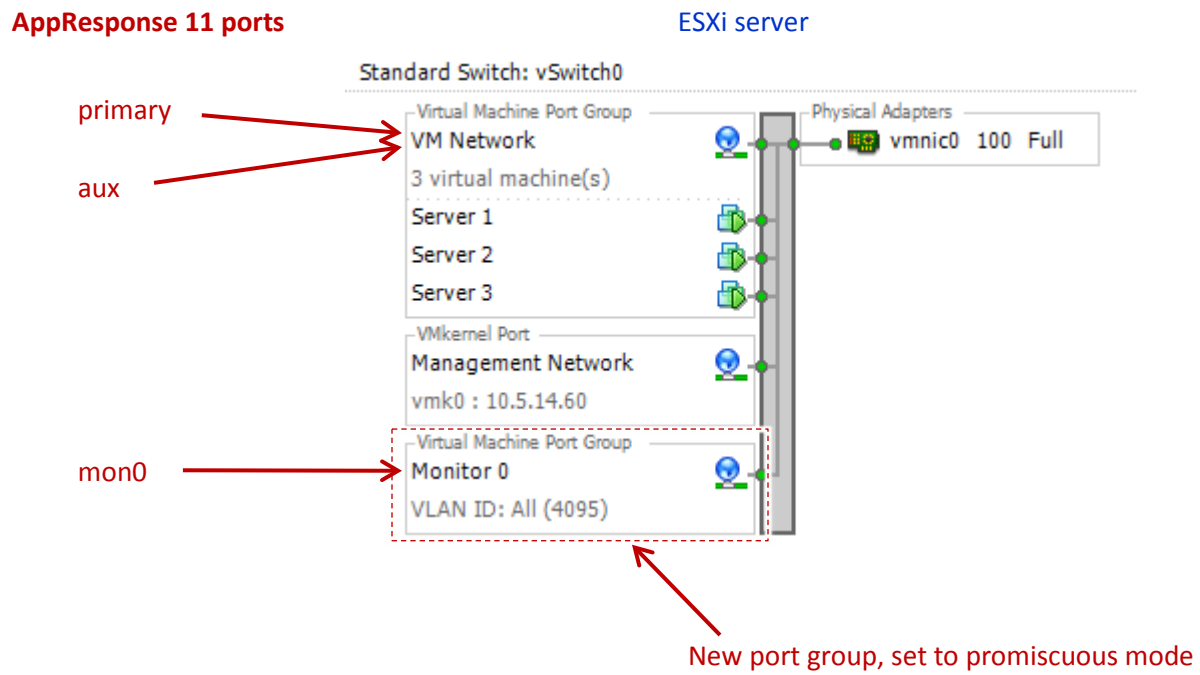
- one additional hard disk for packet storage of size 100GB
- up to three more monitor ports

Before you deploy the AppResponse 11 OVA package, you need to prepare the ESXi server. A typical ESXi server might have a number of application servers running in virtual machines, all located within a single port group (VM Network) on a virtual switch. The diagram below shows these application servers as Server 1, Server 2, and server 3.



When you add AppResponse 11 virtual edition to this ESXi server, **the port group that contains the AppResponse 11 monitor port must be in promiscuous mode, so that the monitor port sees all the traffic on the virtual switch**. Since the promiscuous mode setting applies to an entire port group, and since the port group containing the application servers should be in non-promiscuous mode (the default mode), you need to add a separate port group for the AppResponse 11 monitor port to connect to and set it to promiscuous mode.

During deployment of the OVA package to the ESXi server, you will map the preconfigured ports of the AppResponse 11 to port groups on the virtual switch like this:



Note that the AppResponse 11 management ports, `primary` and `aux`, do not capture data, so they should be in a non-promiscuous-mode port group (VM Network in this example). The monitor port, `mon0`, will be in a promiscuous-mode port group (Monitor0).

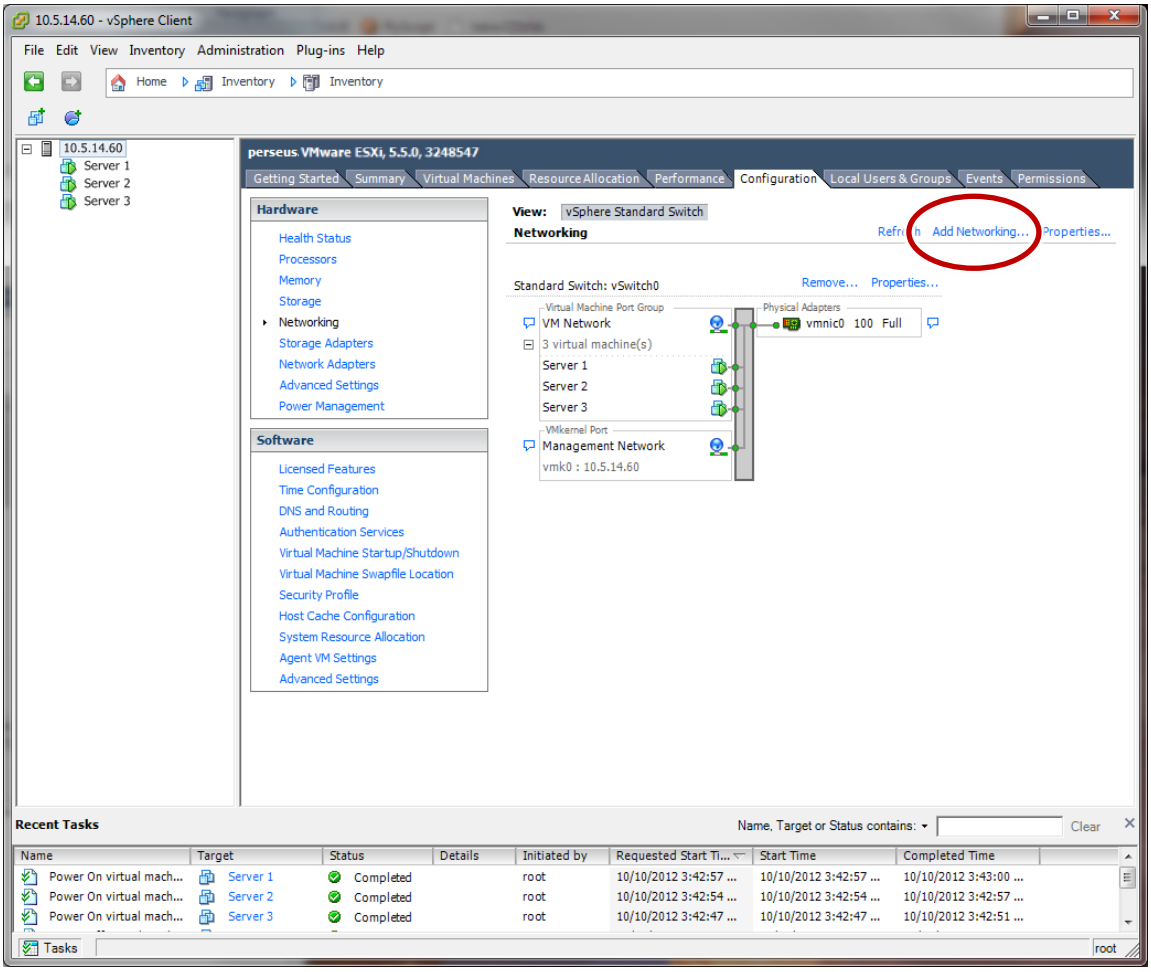
The next two tasks prepare the ESXi server for deployment of the AppResponse 11 OVA package.

- Create a new port group for the monitor port
- Set the new port group to promiscuous mode

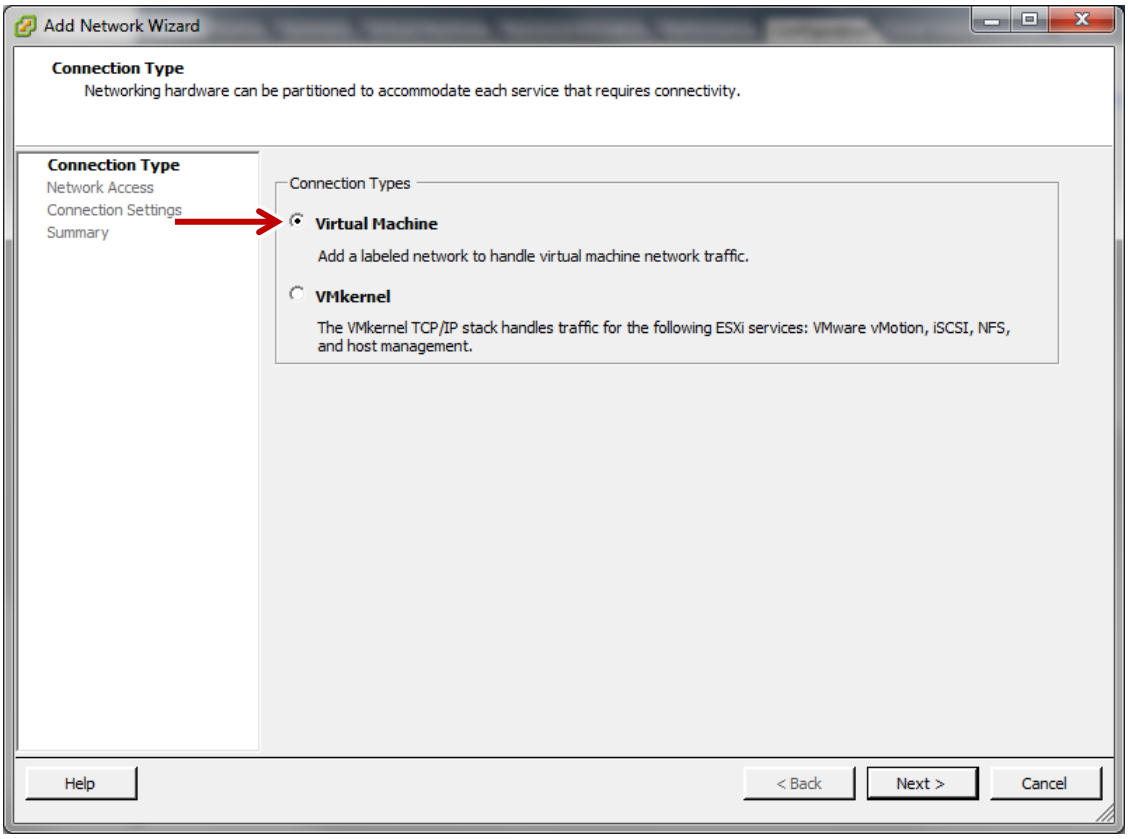
Create a new port group for the monitor port

Create a new port group in the existing virtual switch, vSwitch0.

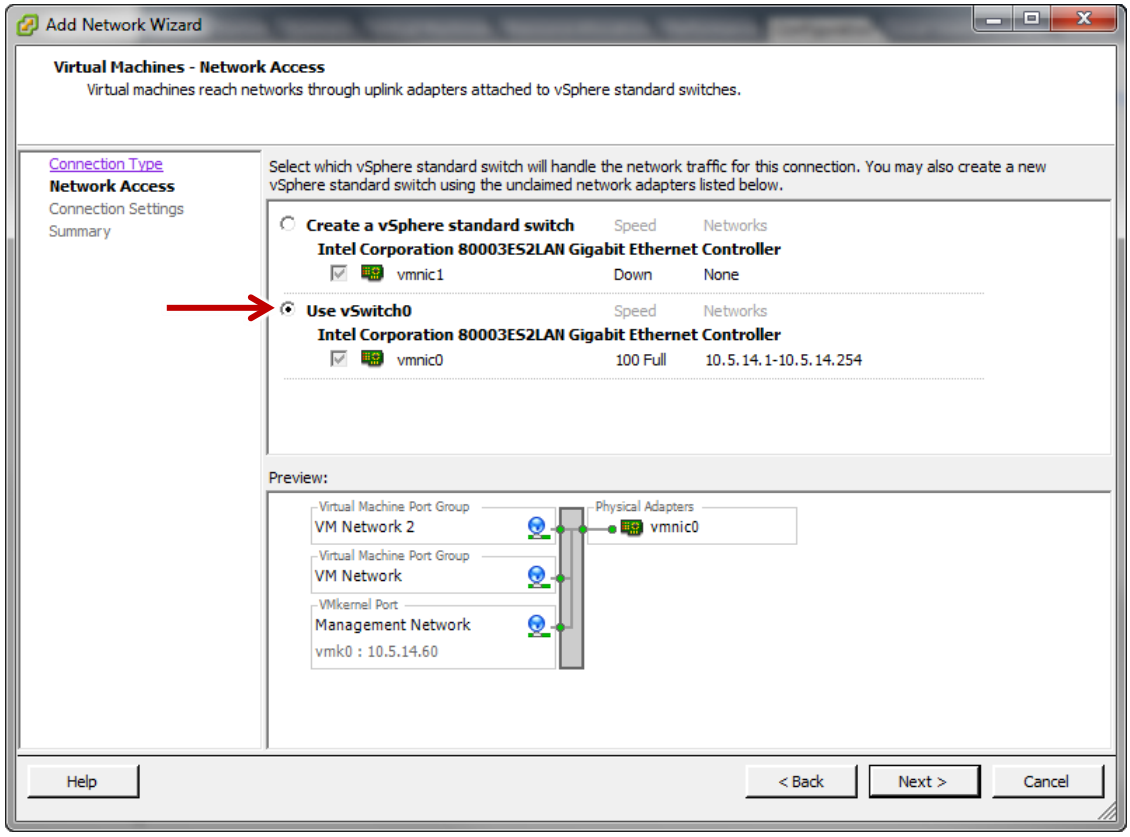
1. In the networking configuration page of the ESXi server, click ***Add Networking…***.



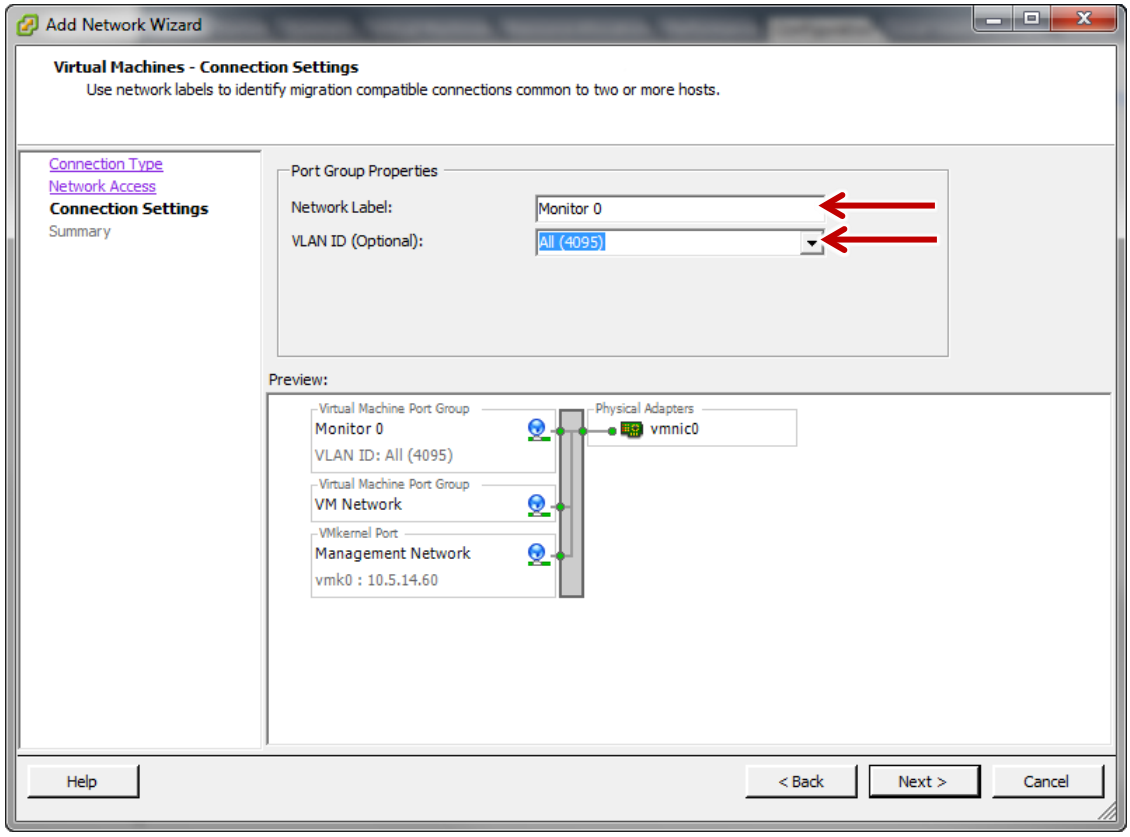
2. Select ***Virtual Machine*** as the connection type.



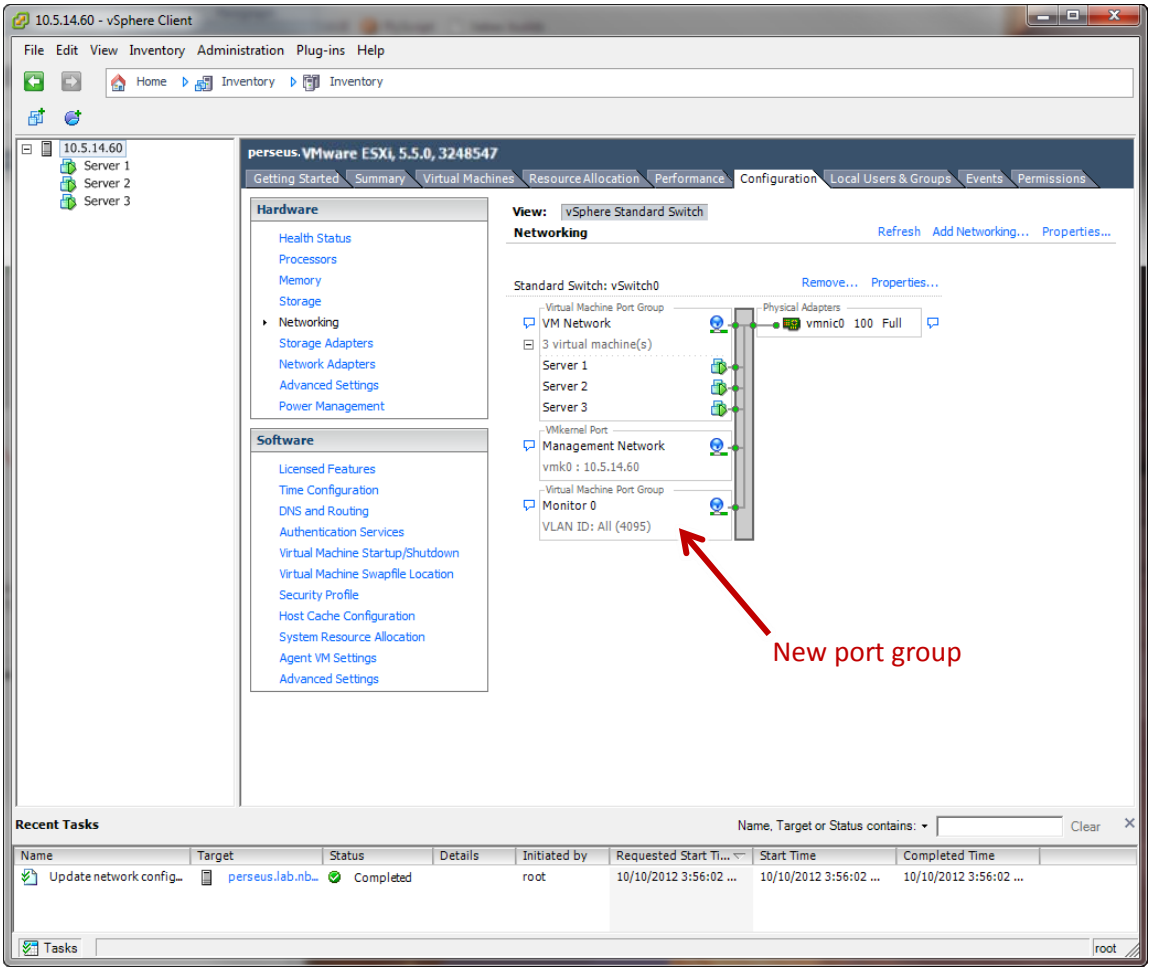
3. Select ***Use vSwitch0***. The ***Preview*** panel at the bottom of the screen shows what the arrangement of port groups on the switch will be.



4. Enter a name for the port group in the ***Network Label*** field. Select a ***VLAN ID*** of ***All (4095)***. This will allow the port group to see all tagged and untagged traffic on the switch.



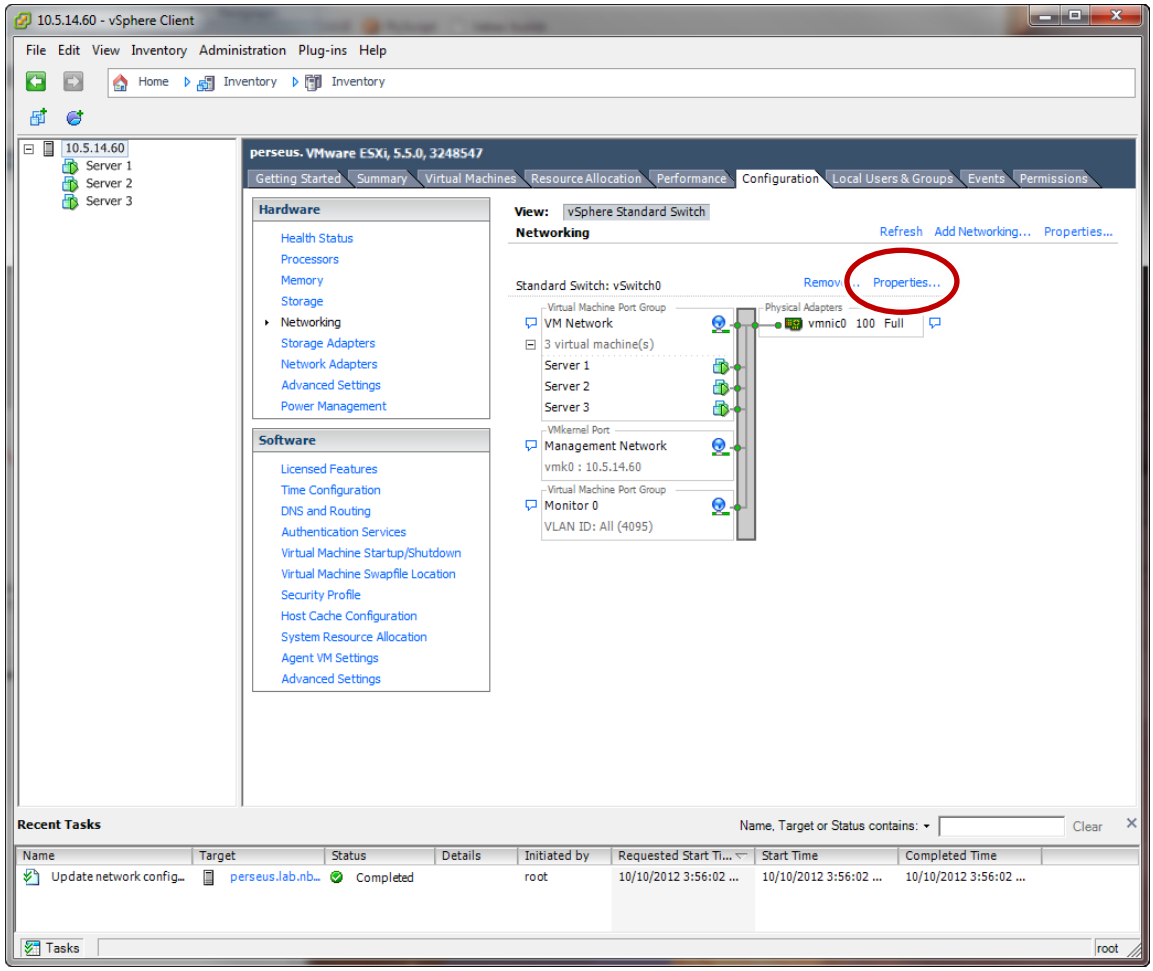
5. On the ***Ready to Complete*** page click ***Finish***. The new port group will be configured on vSwitch0 and the configuration will look like this:



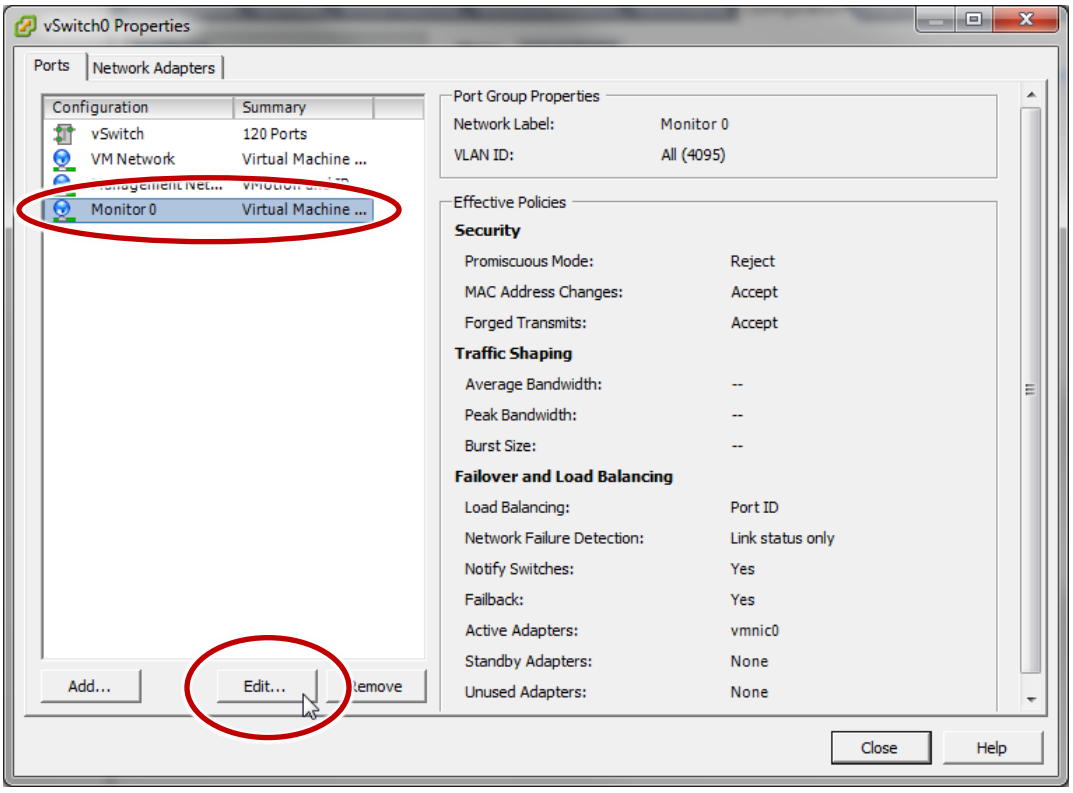
Set the new port group to promiscuous mode

Set the new port group, Monitor0, to promiscuous mode.

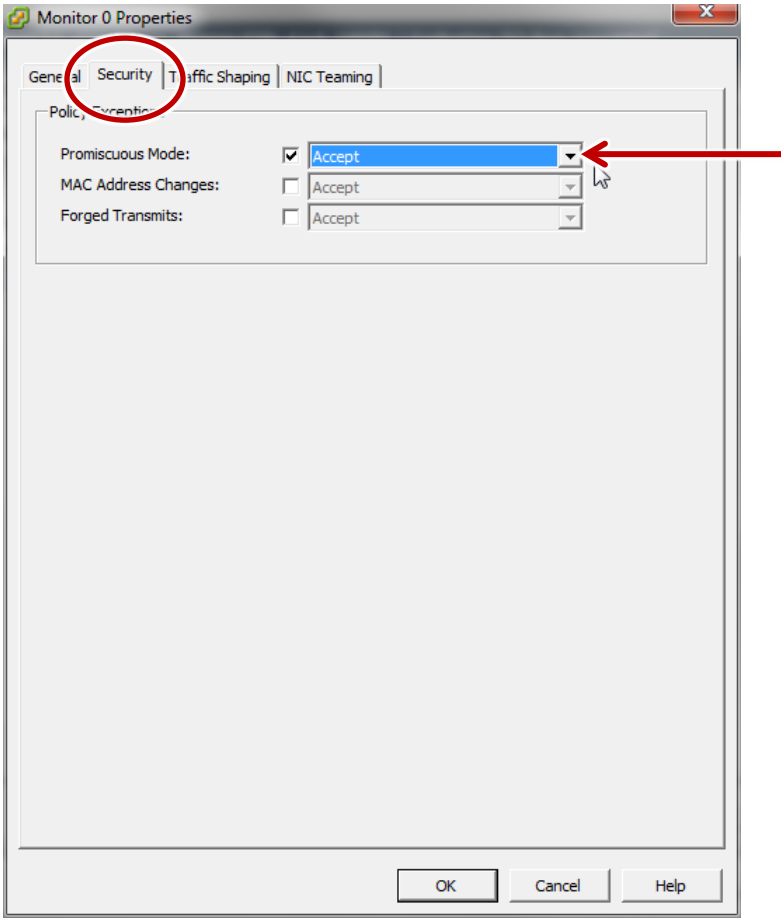
1. In the networking configuration page, click the ***Properties...*** link for vSwitch0.



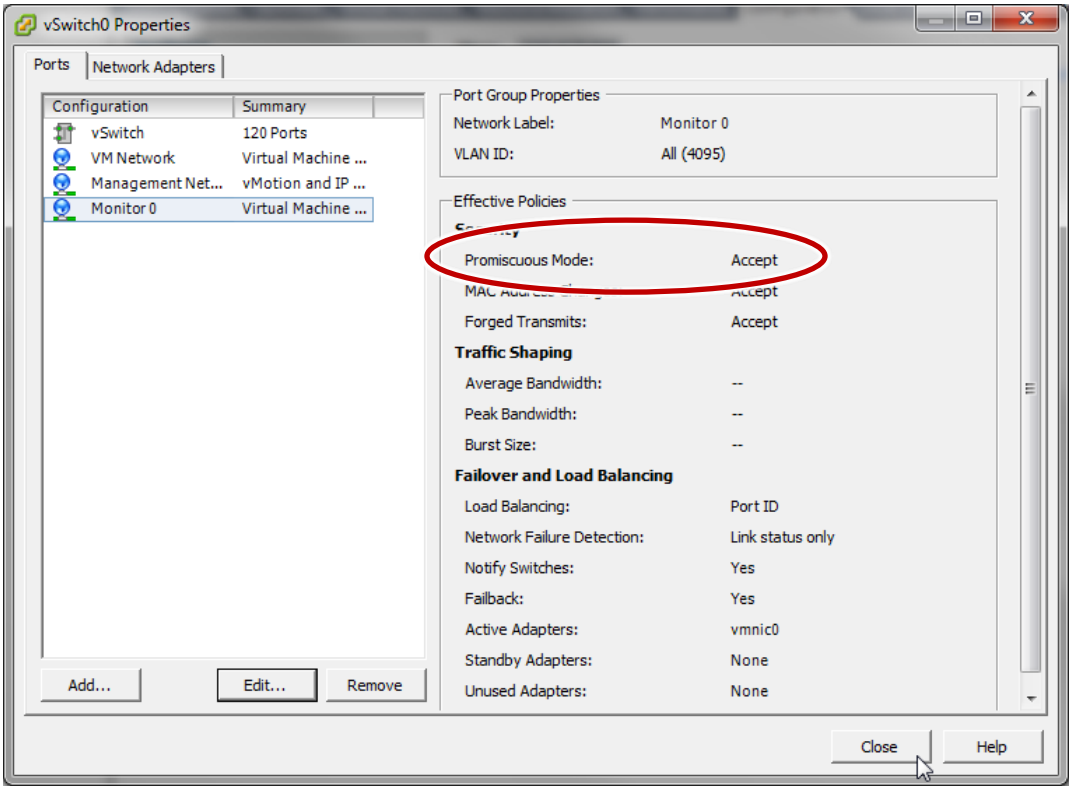
2. Select the ***Monitor0*** port group and click the ***Edit...*** button.



3. Click the ***Security*** tab, check the ***Promiscuous Mode*** check box, and select a value of ***Accept***. Click ***OK***.



4. Verify that ***Promiscuous Mode*** for the Monitor0 port group is set to ***Accept***. Then click ***Close***.



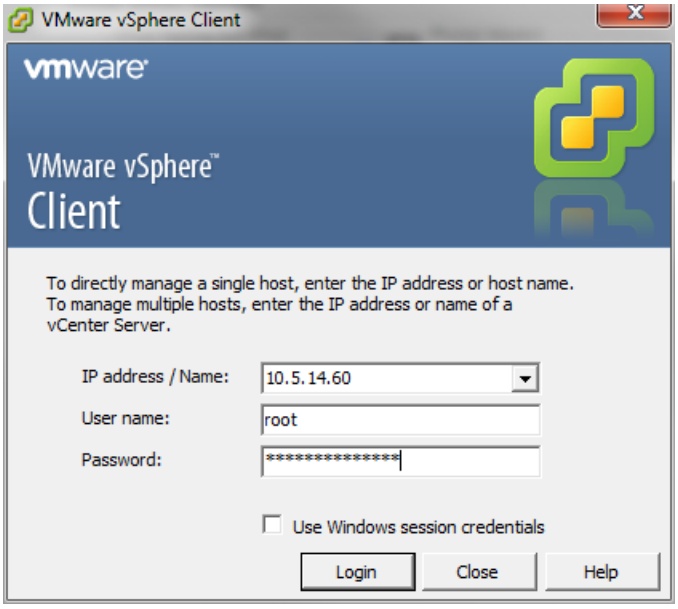
The ESXi server is now prepared for deployment of the AppResponse 11 OVA package.

Deploying AppResponse 11 Virtual Edition

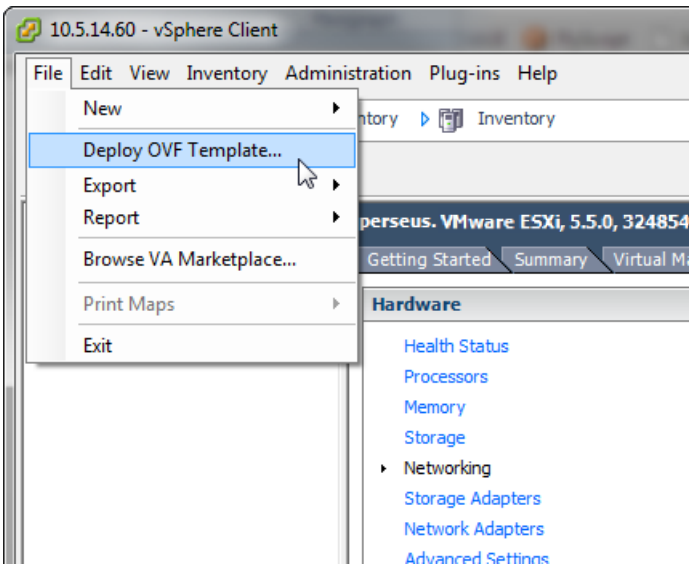
Deploying the AppResponse 11 OVA package to the ESXi server

Install the AppResponse 11 software on the ESXi server, as follows:

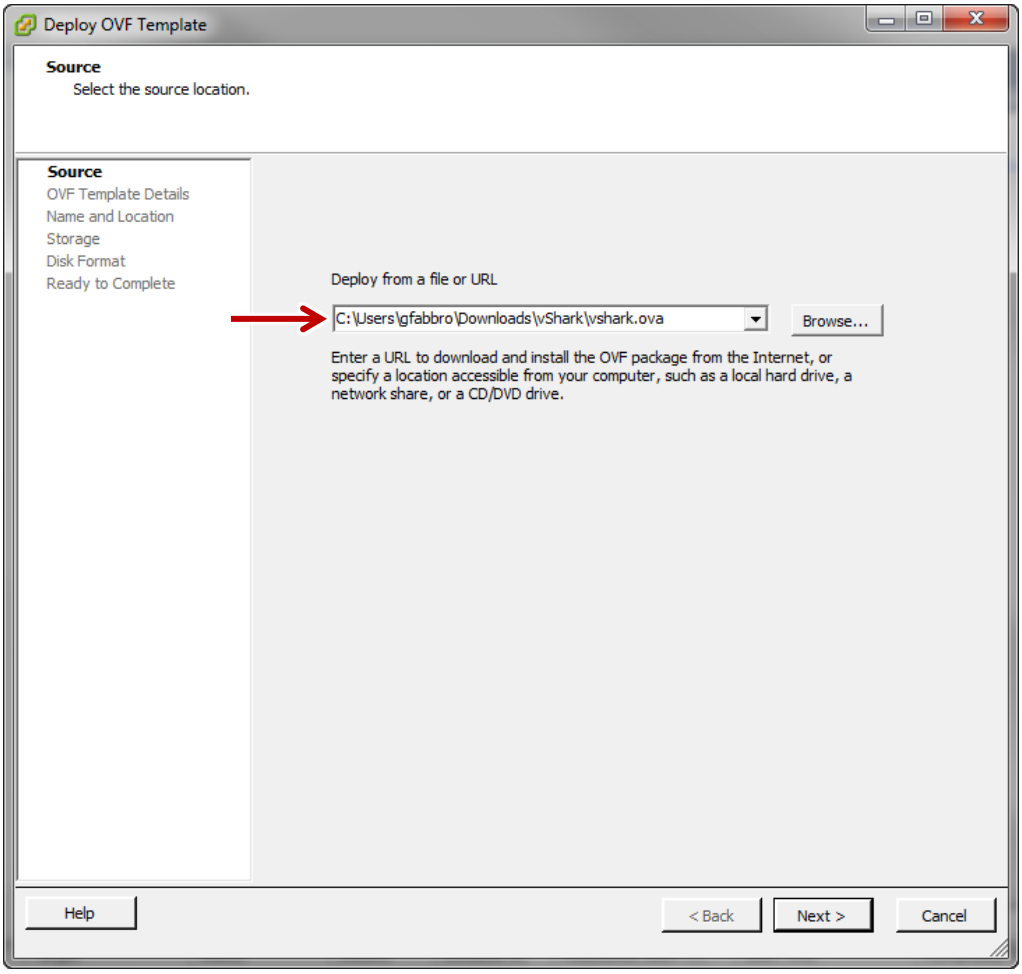
1. Using the VMware vSphere Client, log in to the ESXi server.



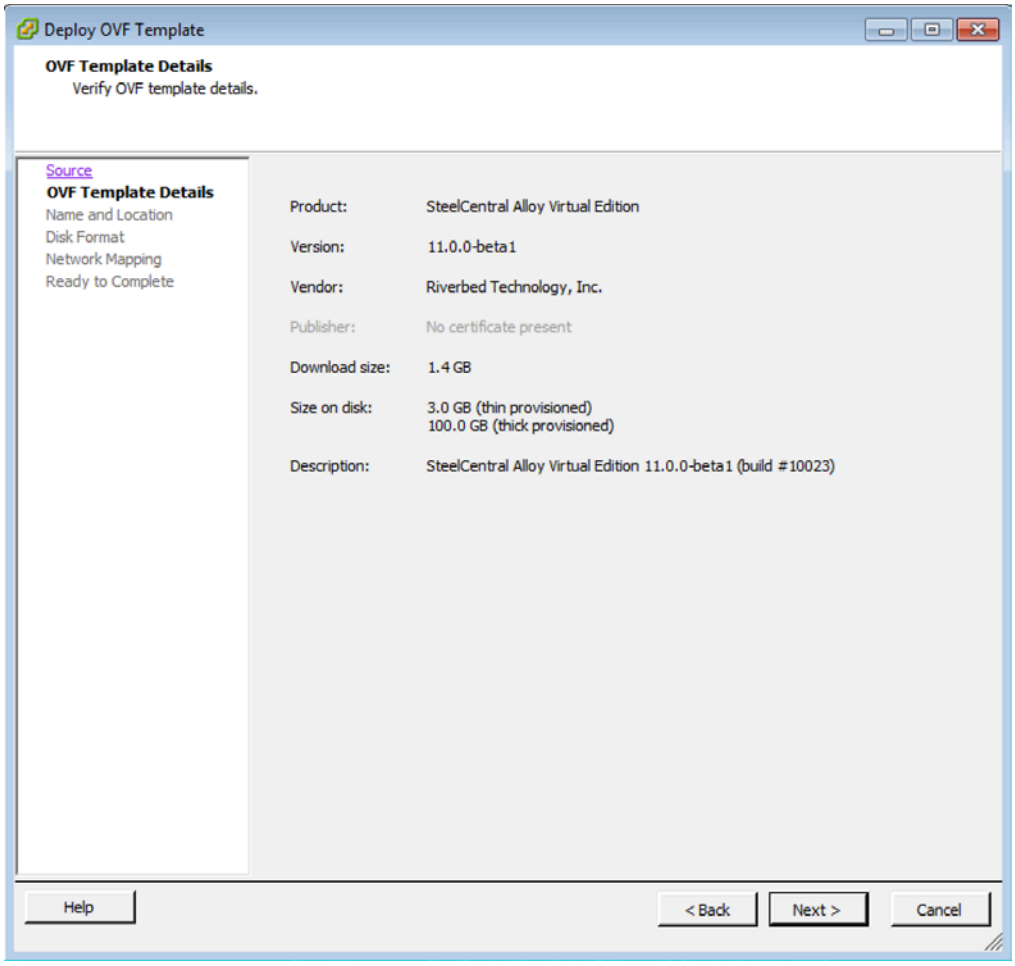
2. Click ***File->Deploy OVF Template…***.



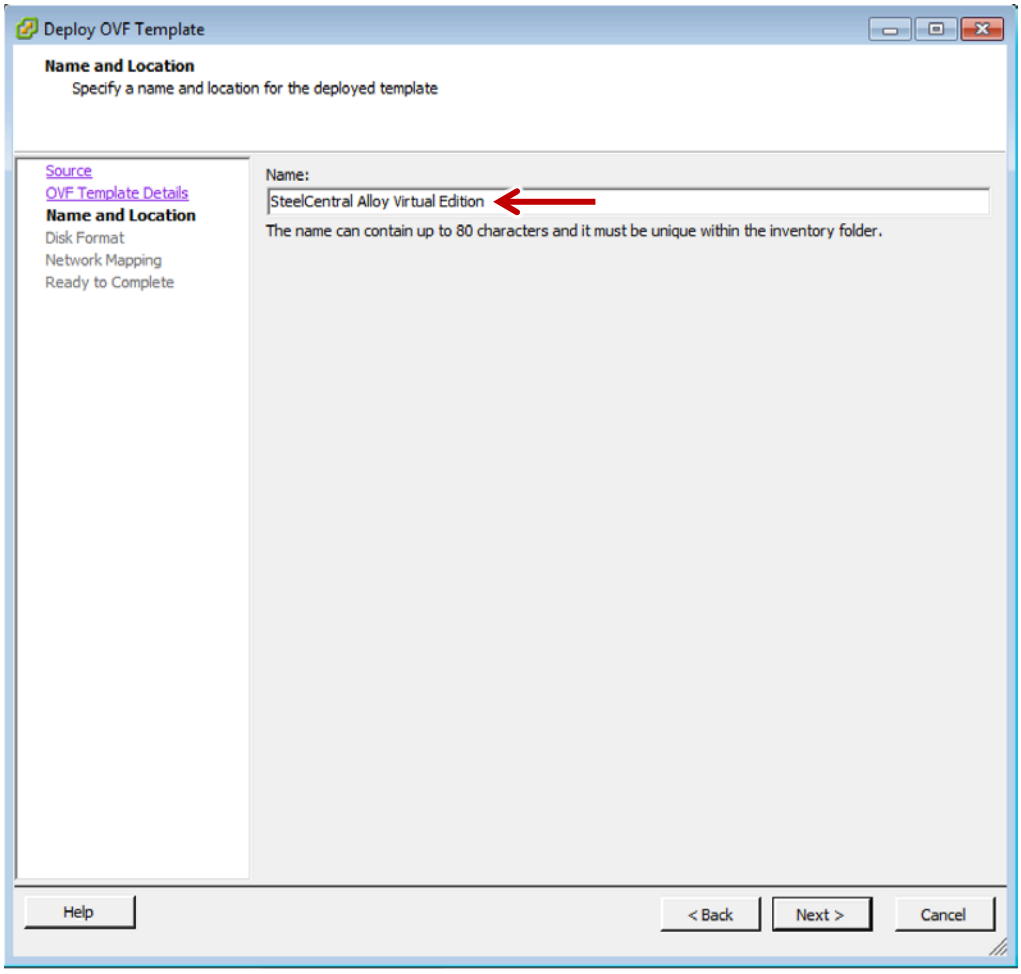
3. On the ***Source*** screen enter the path to the AppResponse 11 OVA file.



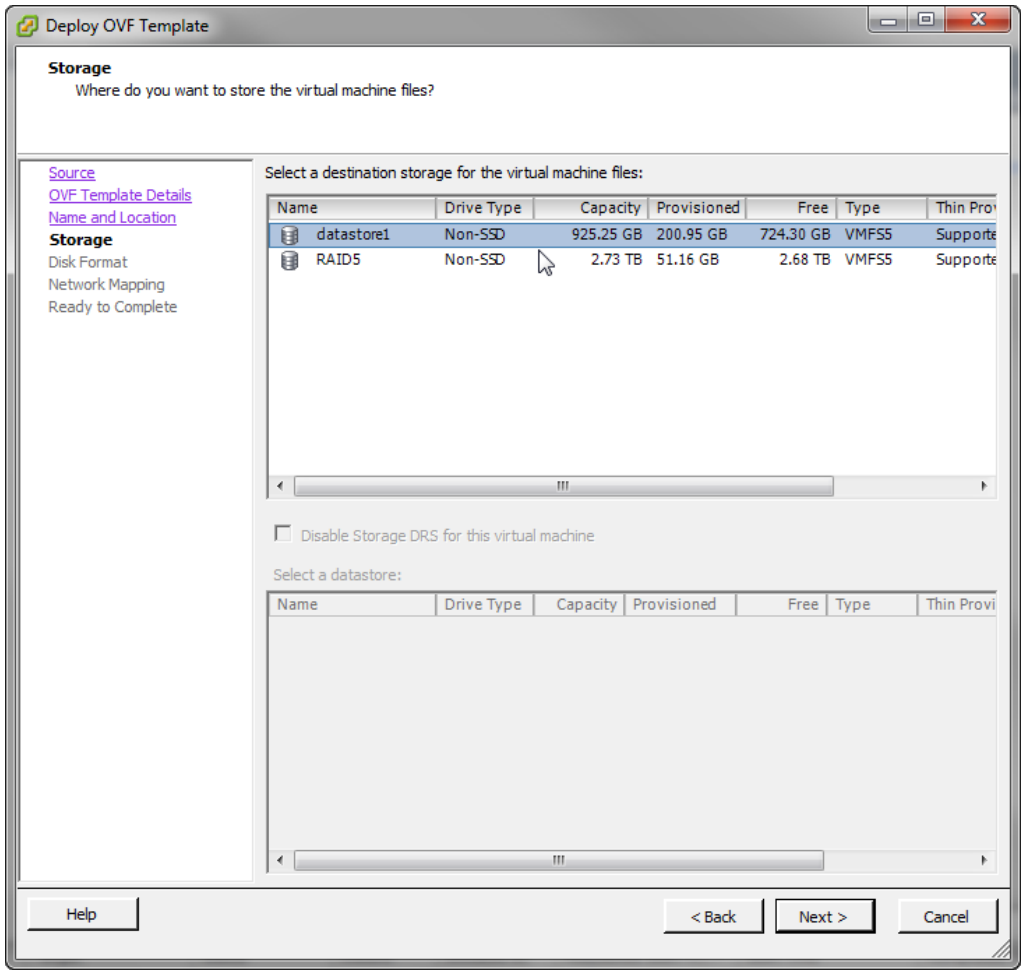
4. On the ***OVF Template Details*** screen, click ***Next***.



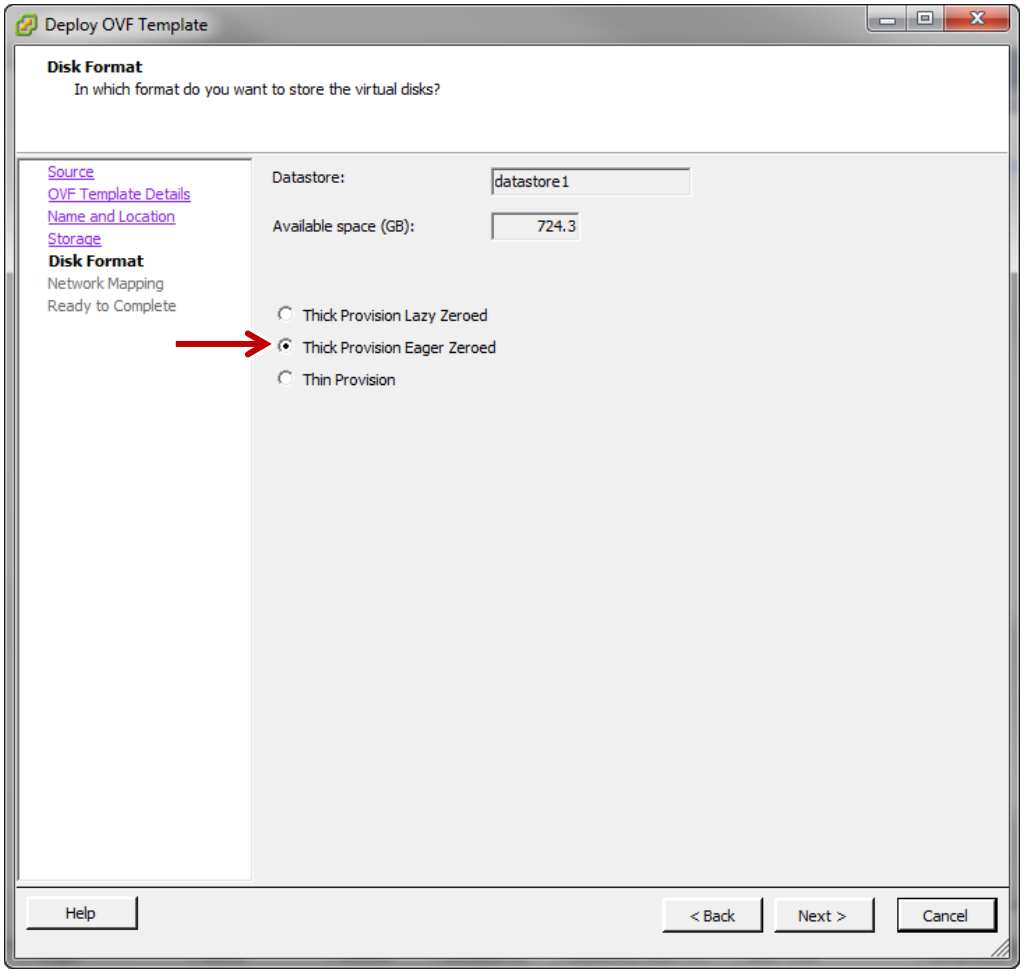
5. On the ***Name and Location*** screen enter a name for the AppResponse 11.



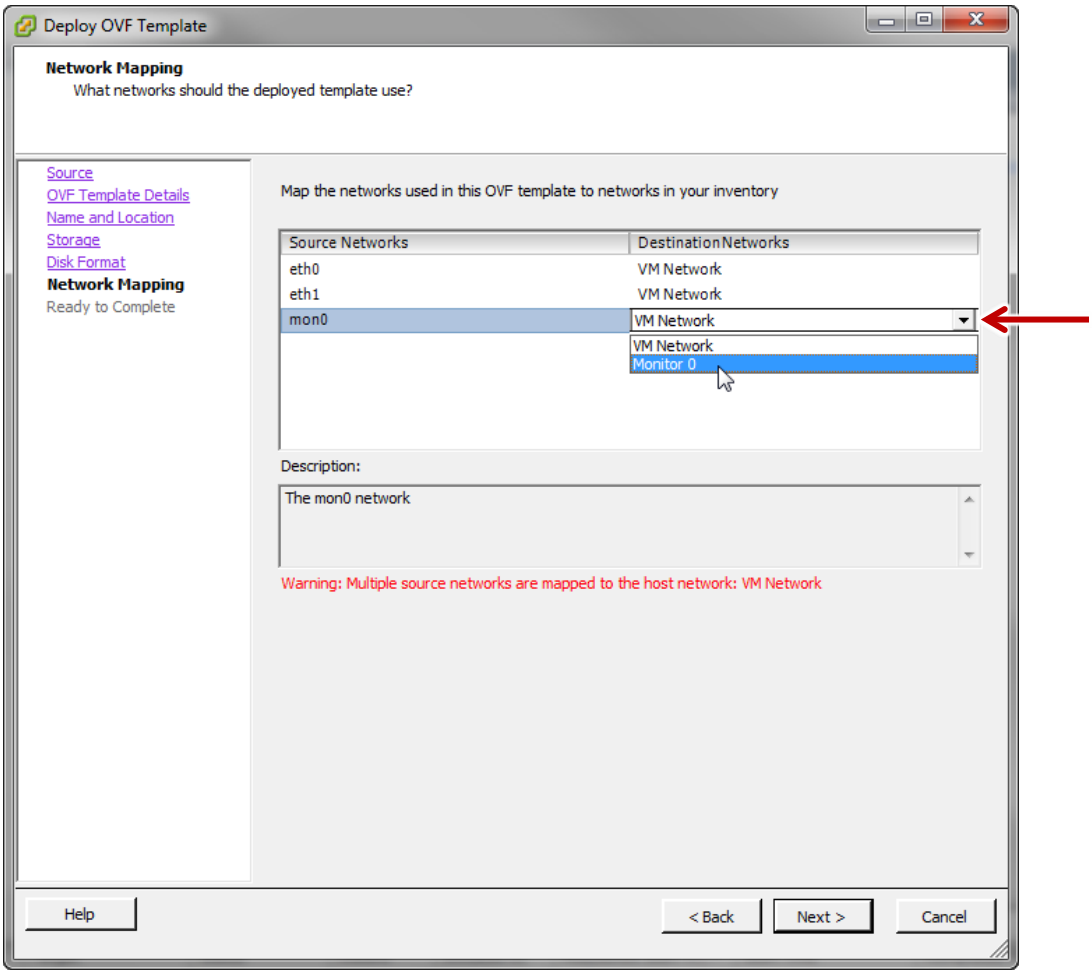
6. On the ***Datastore*** screen, select the server drive where you will store the AppResponse 11 files.



7. On the ***Disk Format*** screen select the disk provisioning form ***Thick Provision Eager Zeroed***.



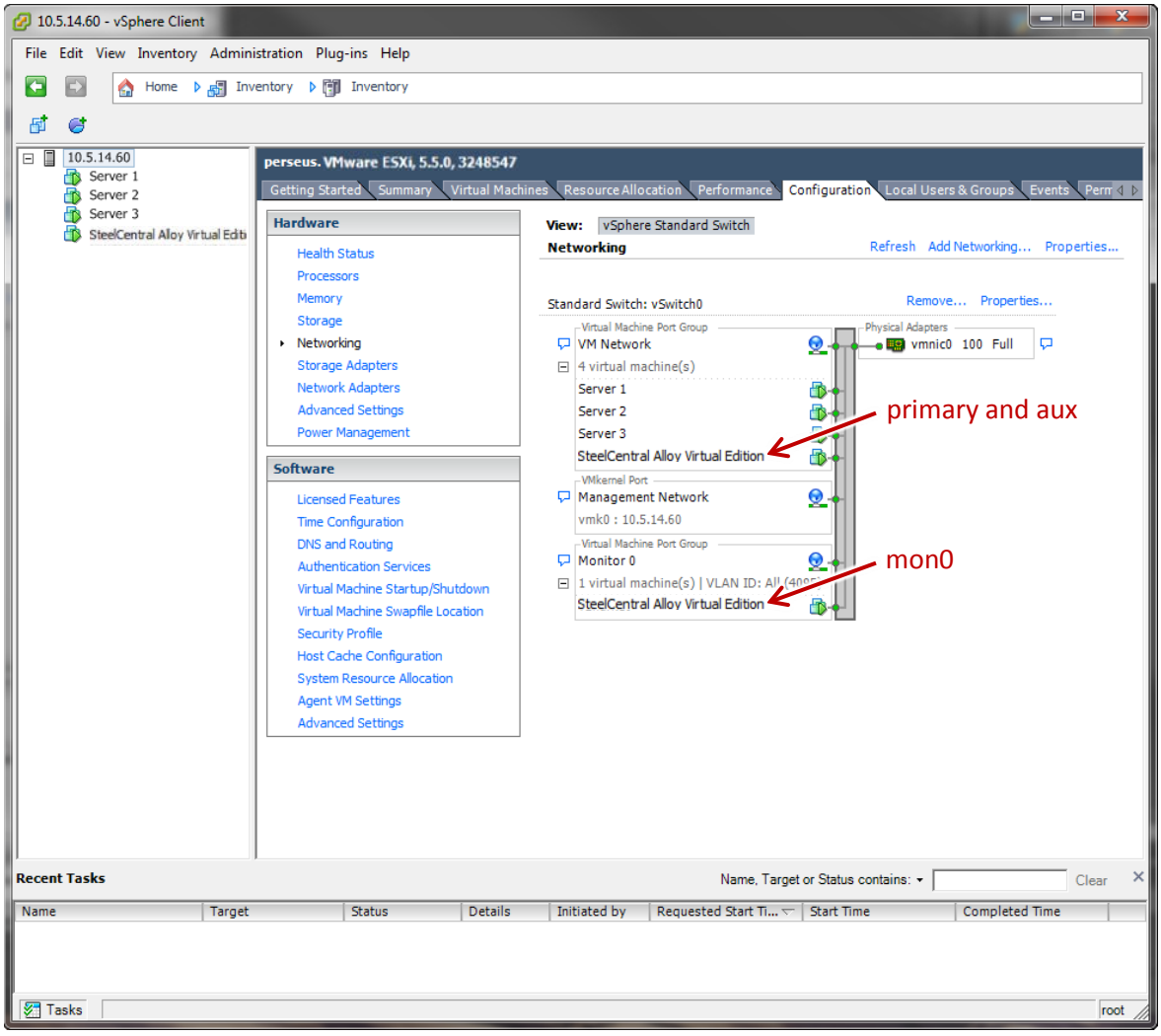
8. On the ***Network Mapping*** page, map the source networks (ports) of the AppResponse 11 to destination networks (port groups) on the server. The `primary` and `aux` source networks are for management; map them to a non-promiscuous-mode destination network (VM Network). The `mon0` source network is for data capture; map it to a promiscuous-mode destination network (Monitor0).



9. On the ***Ready to Complete*** summary page click ***Finish*** to start the deployment.

When the deployment has completed, you can see the resulting network structure on the ***Networking*** configuration page.

In the example configuration shown below, the AppResponse 11 has been added to the server as SteelCentral Alloy Virtual Edition. The `primary` and `aux` ports are mapped to the VM Network port group and the `mon0` port is mapped to the Monitor0 port group.

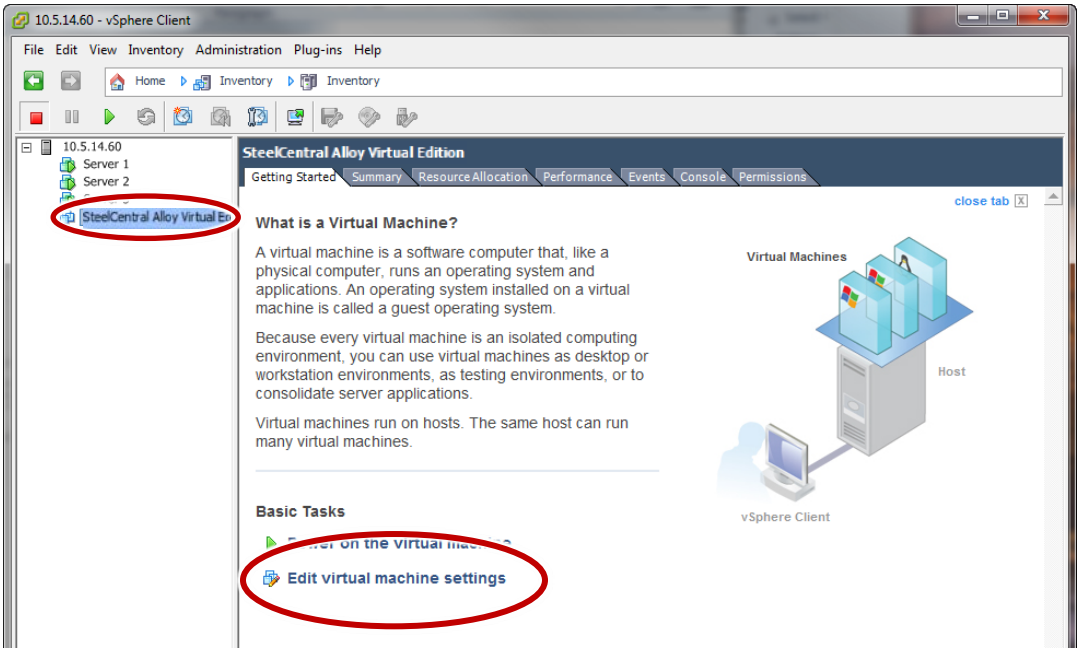


Adding a hard disk

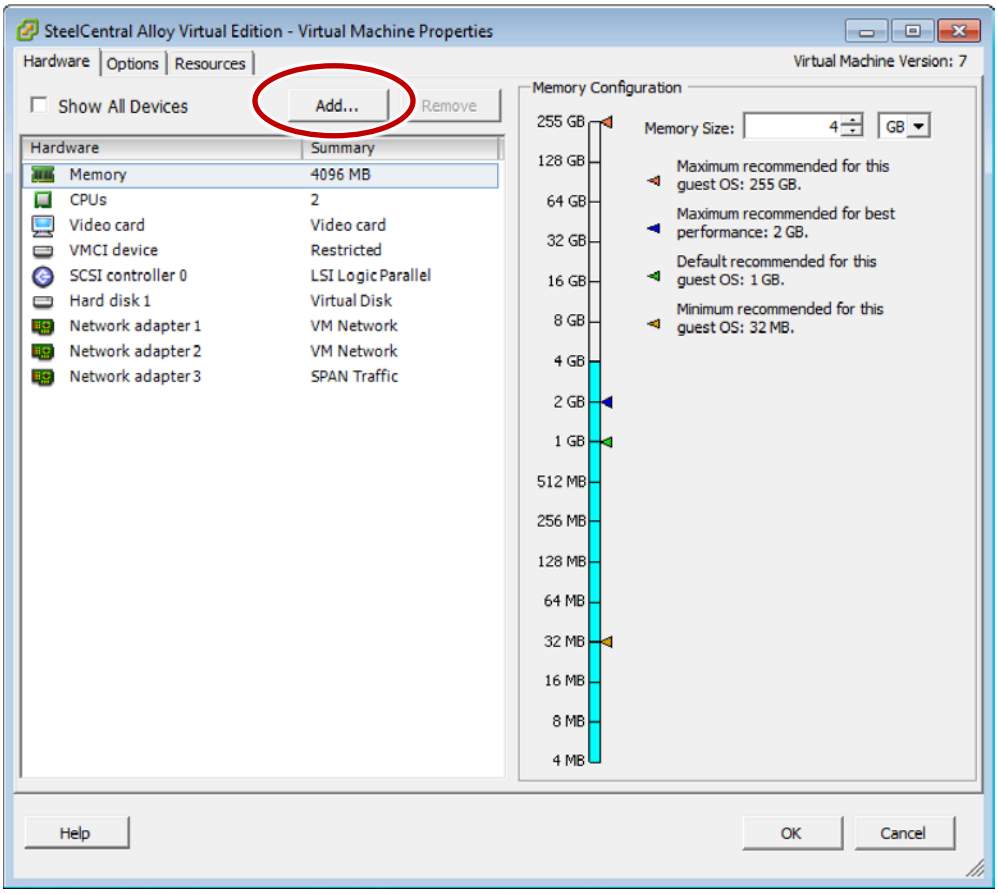
The preconfigured AppResponse 11 has only one hard disk, the operating system disk. To have space for packet storage, you need to configure a second hard disk.

The virtual machine (AppResponse 11) should be powered off before starting this task.

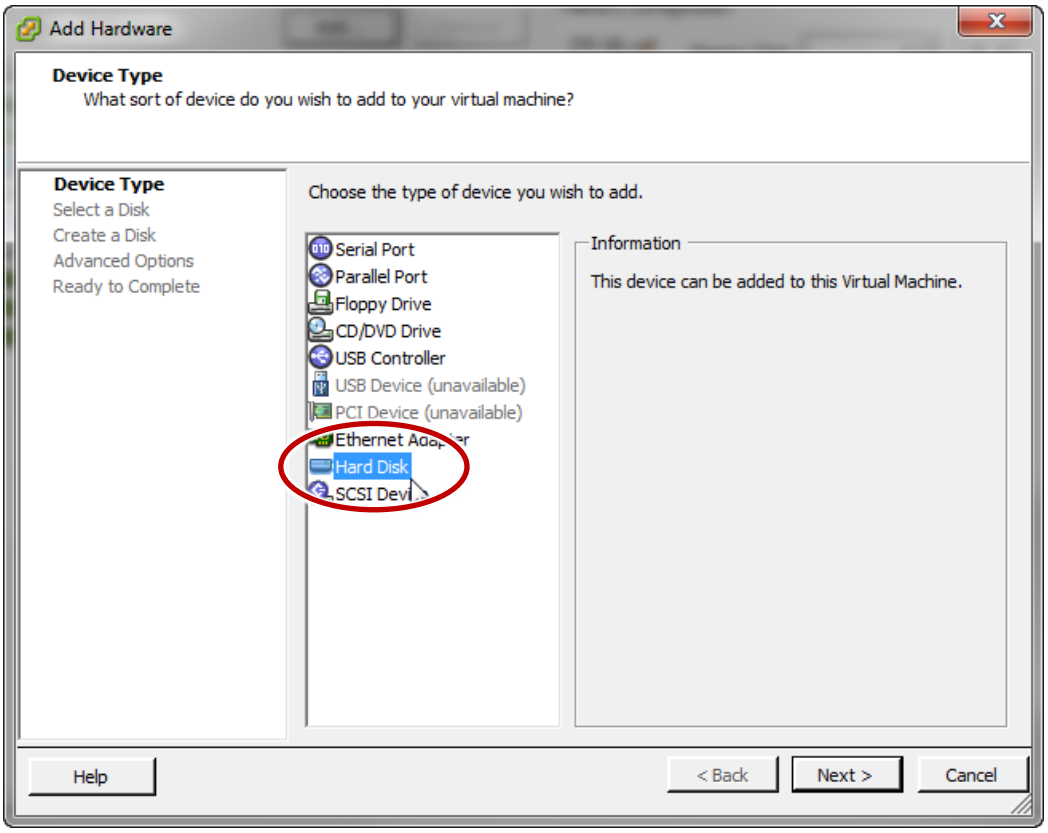
1. Select AppResponse 11 and click ***Edit virtual machine settings***.



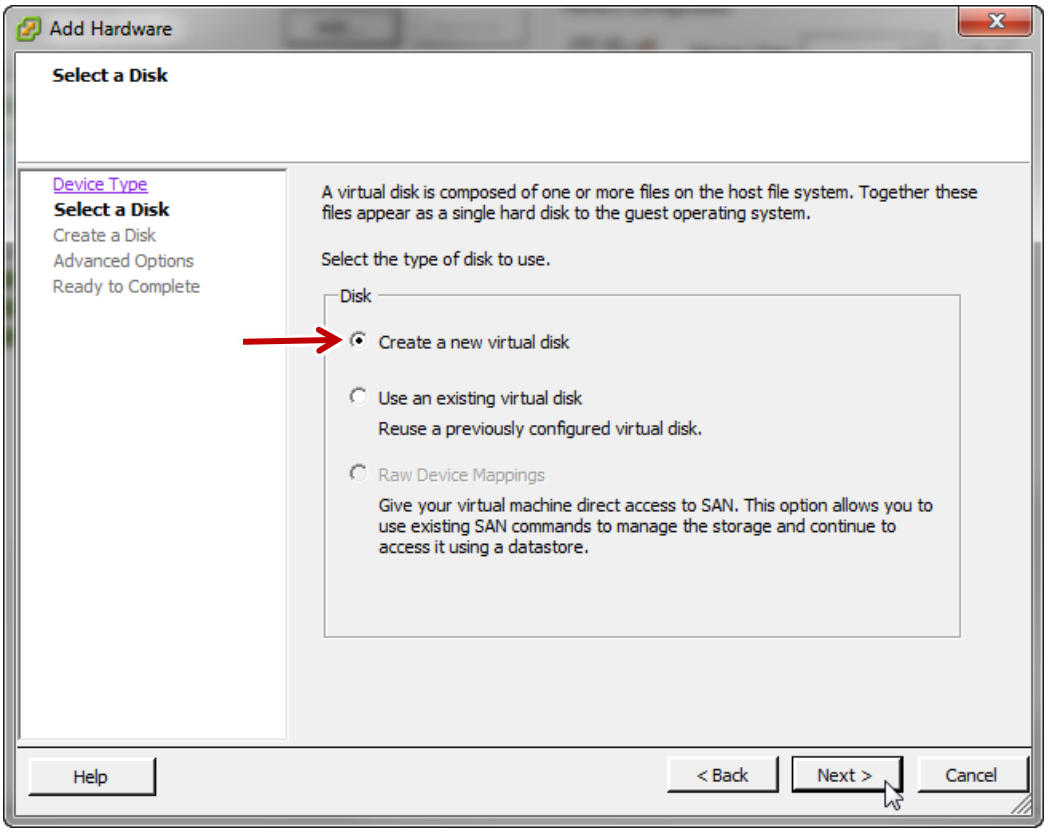
2. Click ***Add...***.


SteelCentral Alloy Virtual Edition - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 7
Show All Devices
Add...
Remove
Hardware
Summary
Memory
4096 MB
CPUs
2
Video card
Video card
VMCI device
Restricted
SCSI controller 0
LSI Logic Parallel
Hard disk 1
Virtual Disk
Network adapter 1
VM Network
Network adapter 2
VM Network
Network adapter 3
SPAN Traffic
Memory Configuration
Memory Size:
4
GB
255 GB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended for this guest OS: 255 GB.
Maximum recommended for best performance: 2 GB.
Default recommended for this guest OS: 1 GB.
Minimum recommended for this guest OS: 32 MB.
Help
OK
Cancel

3. On the ***Device Type*** page select ***Hard Disk***.



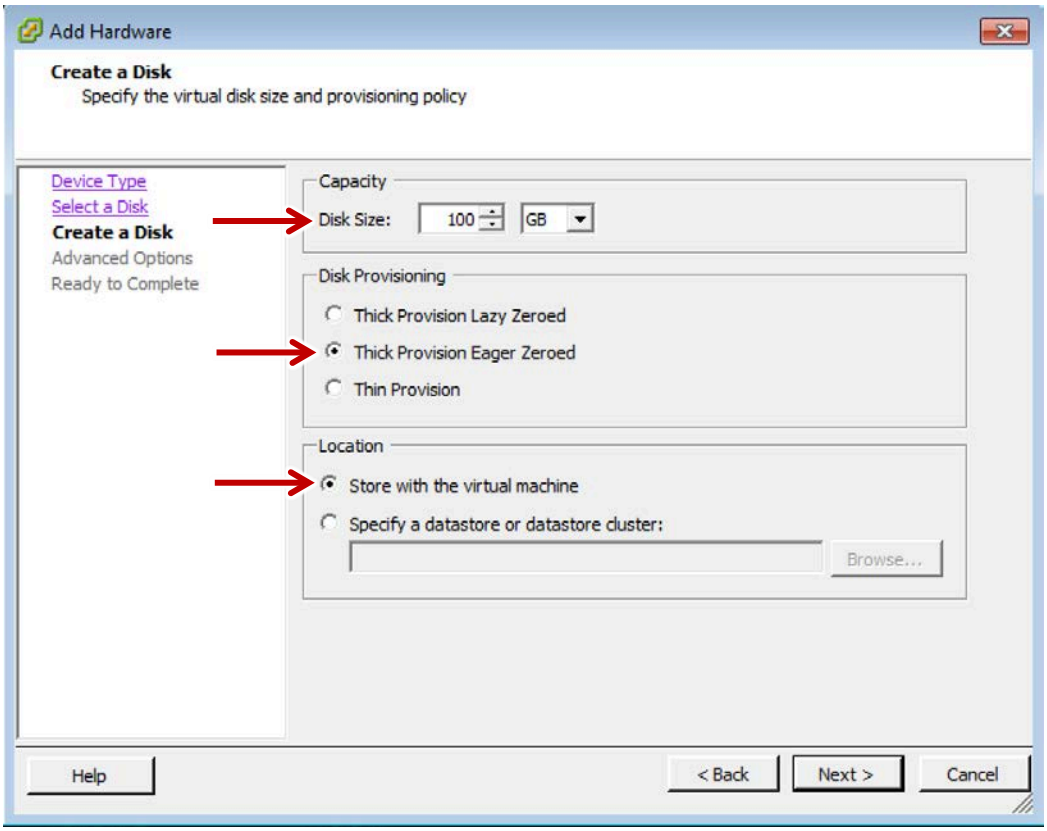
4. On the ***Select a Disk*** page select ***Create a new virtual disk***.



5. On the ***Create a Disk*** page, enter a size of 100GB for the packet storage disk.

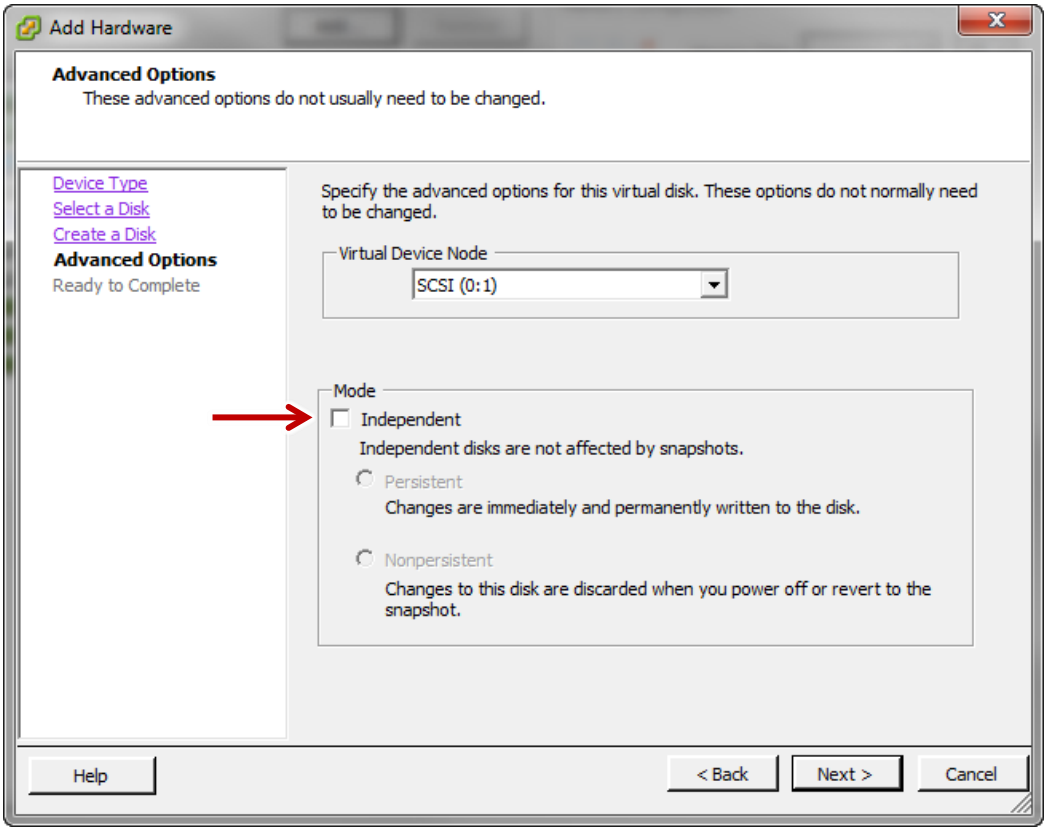
   For disk provisioning, select ***Thick Provision Eager Zeroed***.

   You can choose to store the disk with the virtual machine, or you can choose a different datastore.



6. On the ***Advanced Options*** page, accept the default setting for ***Virtual Device Node***. Check that that the ***Mode*** settings are the same as for the OS disk. By default, the OS disk is **not** set to independent mode.

   You can find the OS disk's mode settings as follows:
   (1) From the vSphere Client main page select the AppResponse 11.
   (2) Click the "Getting Started" tab.
   (3) Click "Edit virtual machine settings".
   (4) Click the OS disk in the Hardware list—usually "Hard disk 1".
   The mode settings appear in the panel on the right.



7. On the ***Ready to Complete*** page, click ***Finish*** to create the hard disk.

8. The ***Virtual Machine Properties*** page shows the new hard disk ready to be added. Click ***OK*** to add it.

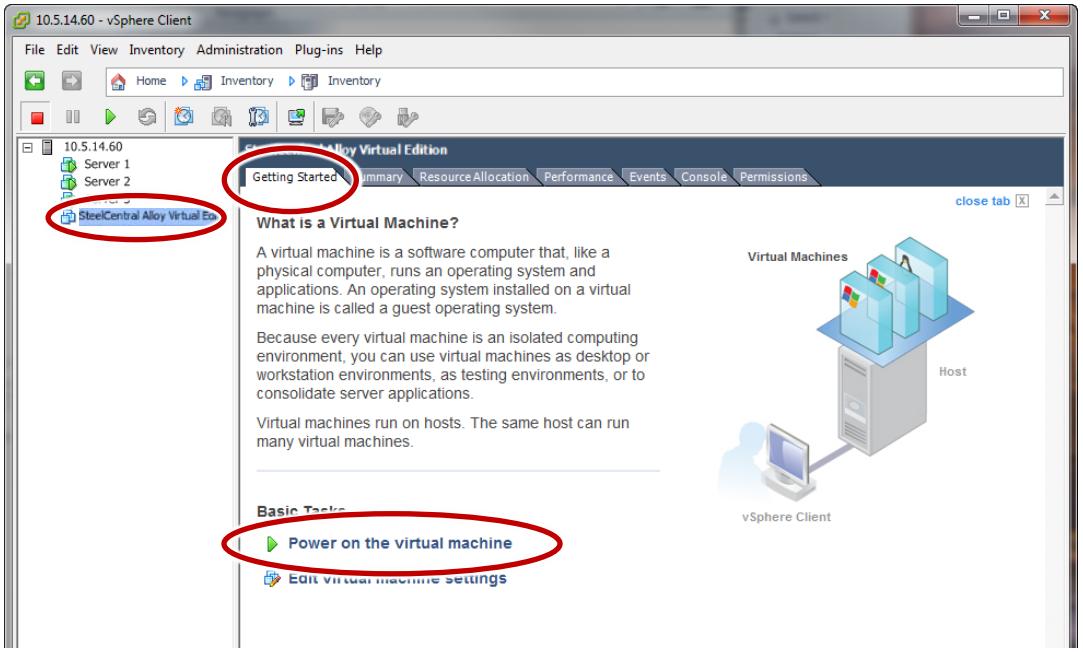
When you have added the hard disk and set up all your monitor ports, you are finished creating the AppResponse 11. Continue with the next chapter to configure it for use in your network.

Configuring AppResponse 11 Virtual Edition

Setting up the initial configuration

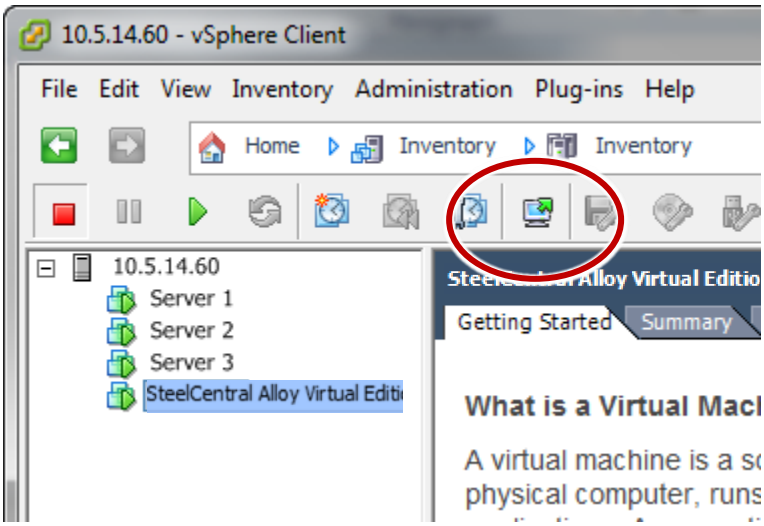
The initial configuration sets up the AppResponse 11 so its web UI is accessible by a web browser. You perform this configuration through the AppResponse 11 console port.

1. Power on the AppResponse 11. Select the AppResponse 11 icon from the server's list of virtual machines. Click the ***Getting Started*** tab, then click ***Power on the virtual machine***.



The AppResponse 11 icon in the list of virtual machines adds a green arrowhead to indicate that it is powered on.

2. Click the console button to launch the AppResponse 11 console.



Note: If you lose the mouse cursor while working in the console interface, you can restore it by entering **Ctrl+Alt**.

3. At the **login:** prompt, enter the default username and password.
   `login:` **admin**
   `password:` **admin**
   See "Changing the default password" for more information.
4. At the console prompt, enter **enable**, **configure terminal**, and **wizard**, to start the initial configuration wizard, and answer the questions.

```
localhost > enable
localhost # configure terminal
localhost (config) # wizard
```

The setup wizard guides you through the initial configuration of the appliance. Press **Enter** at any step to accept the current setting "[ ]" and move to the next step. For example:

```
---------------------------------------
Hostname [localhost]: localhost
Primary interface DHCP enabled [yes]: no
Primary interface IP address []: 192.168.1.100
Primary interface subnet mask []: 255.255.255.0
Aux interface enabled [no]: no
Default gateway []: 192.168.1.1
DNS servers (comma-separated IPv4 addresses) []: 192.168.1.1
DNS domain names (comma-separated) []: example.com
```

```
Timezone [America/Los_Angeles]: America/Los_Angeles (* for list)

You have entered the following configuration:
 1: Hostname: localhost
 2: Primary interface DHCP enabled: no
 3: Primary interface IP address: 192.168.1.100
 4: Primary interface subnet mask: 255.255.255.0
 5: Aux interface enabled: no
 6: Default gateway: 192.168.1.1
 7: DNS servers (comma-separated IPv4 addresses): 192.168.1.1
 8: DNS domain names (comma-separated): example.com
 9: Timezone: America/Los_Angeles

To change an answer, enter the step number to return to
Enter 'save' to save changes and exit
Enter 'quit' to quit without changing
```

Enter '`save`' to save changes, quit to exit, or enter an item number in the list to edit it.

If you have used DHCP to provision an IP address for AppResponse 11, at the console prompt enter **`show interfaces primary`** to find the IP address.

```
Local host (config) # show interfaces primary
Interface primary state:
    Up:                    yes
    Interface type:        Ethernet
    DHCP enabled:          yes
    IP address:            10.33.159.73
    Netmask:               255.255.255.0
    DHCPv6 enabled:        no
    Link-local address: ffff::250:56ff:fe88:a672/64
    Speed:                 10000 Mbit/Sec
    Duplex:                full
    MTU:                   1500
    HW address:            00:50:56:ff:a6:72
    Link:                  yes
local host (config) #
```

You will use this address (or the DNS name of the AppResponse 11) to connect to the web user interface for subsequent configuration and operation of the AppResponse 11.

Signing in to the AppResponse 11 web user interface

The web user interface (web interface) is a primary means of access to the AppResponse 11. You use it for further configuration of the AppResponse 11, as well as for normal operation.

Connect to the AppResponse 11 through its web user interface using your web browser. The AppResponse 11 web interface is supported on Internet Explorer 11, Mozilla Firefox ESR 45, and Google Chrome 51 browsers.

Note: Make sure that SSL, cookies, and JavaScript are enabled in your browser

1. Point your browser to https://<AppResponse 11IP> where <AppResponse 11IP> is the IP address of the AppResponse 11 virtual edition.
2. Enter username and password, then click the login button. (Default value is 'admin' for both username and password)

Licensing

An AppResponse virtual edition requires a license to collect and analyze network traffic. When you purchase an AppResponse virtual edition or an upgrade, Riverbed sends an email to your Support account username containing the Product Key. The Product Key is used to install the license and the Feature Keys that:

- Allow the AppResponse 11 appliance to operate.
- Enable the licensed capabilities and capacities, for example, a Web Transaction Analysis add-on module.

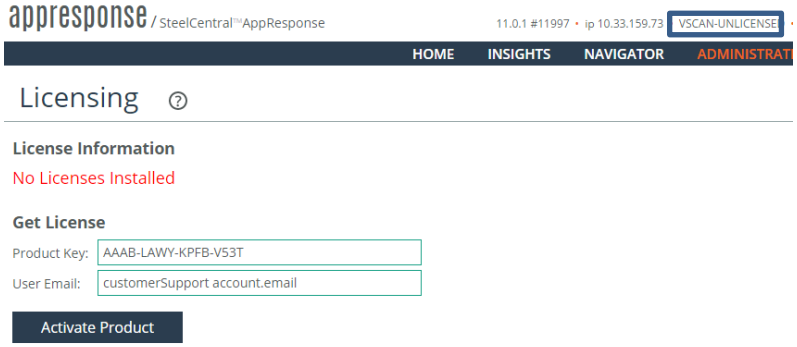
Important: An AppResponse 11 virtual edition license is installed using a Product Key. The license is for that Product Key and can only be used with that Product Key. A Product Key can be activated and deactivated through the AppResponse web interface. During deactivation, a deactivation code is created that can be used by the License provider to produce a new Product Key to license another virtual edition.

A product key can be used on the Licenses page of the Riverbed Support site (https://licensing.riverbed.com) to view and manage your licenses. For more information on licenses, see Licensing in the *AppResponse 11 User's Guide* or the AppResponse 11 web UI Help.

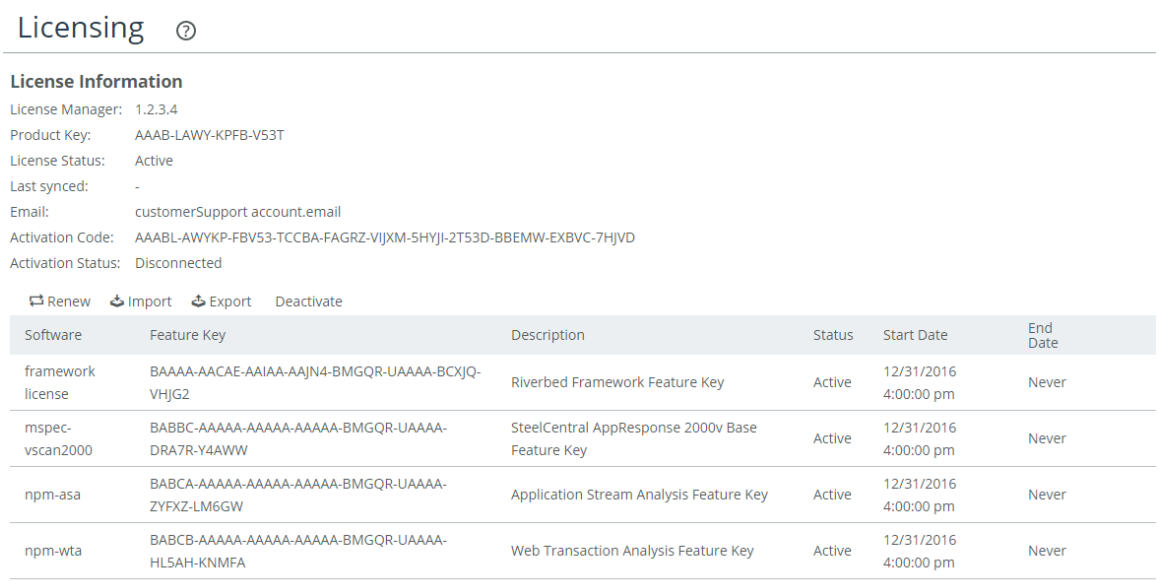
Licensing a Virtual Edition with an Internet Connection

The header line at the top of each AppResponse 11 web UI page shows the AppResponse 11 model and license. If no license is installed "UNLICENSED" is displayed after the model.

1. In the AppResponse 11 web UI go to Administration > Other: Licensing.
2. Enter the Product Key.
3. Enter the Email address of the user activating the license.



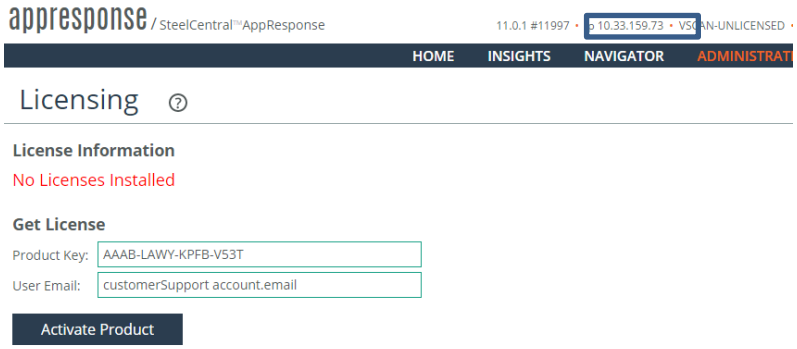
4. Click **Activate Product**. No further action is required. AppResponse automatically opens a connection over the Internet to the Riverbed Licensing site. A valid license is activated and the Feature Keys are installed automatically.



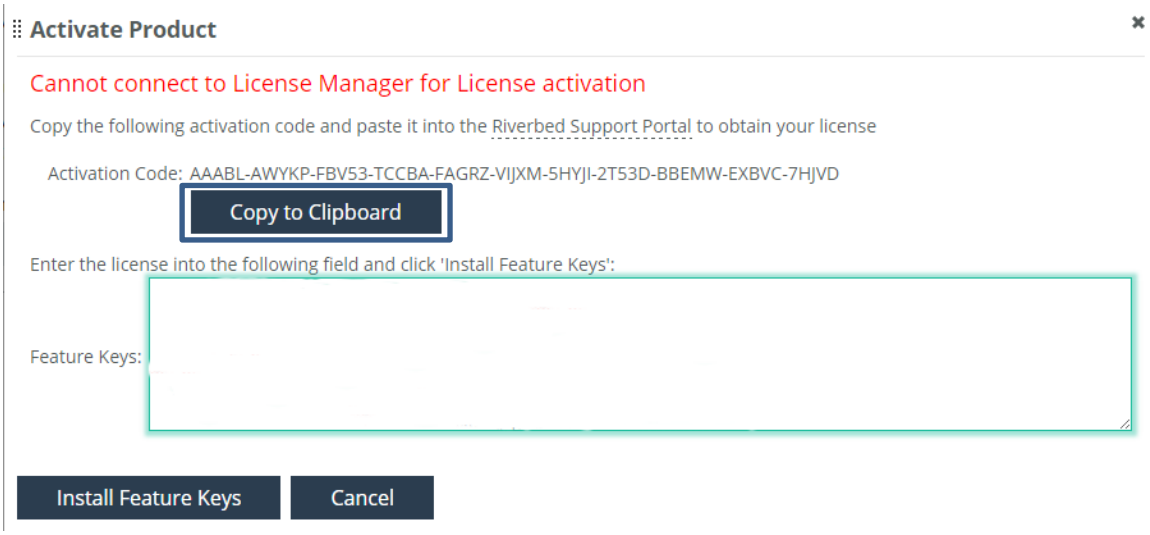
Software	Feature Key	Description	Status	Start Date	End Date
framework license	BAAAA-AACAE-AAIAA-AAJN4-BMGQR-UAAAA-BCXJQ-VHJG2	Riverbed Framework Feature Key	Active	12/31/2016 4:00:00 pm	Never
mspec-vscan2000	BABBC-AAAAA-AAAAA-AAAAA-BMGQR-UAAAA-DRA7R-Y4AWW	SteelCentral AppResponse 2000v Base Feature Key	Active	12/31/2016 4:00:00 pm	Never
npm-asa	BABCA-AAAAA-AAAAA-AAAAA-BMGQR-UAAAA-ZYFXZ-LM6GW	Application Stream Analysis Feature Key	Active	12/31/2016 4:00:00 pm	Never
npm-wta	BABCB-AAAAA-AAAAA-AAAAA-BMGQR-UAAAA-HL5AH-KNMFA	Web Transaction Analysis Feature Key	Active	12/31/2016 4:00:00 pm	Never

Licensing a Virtual Edition with No Internet Connection

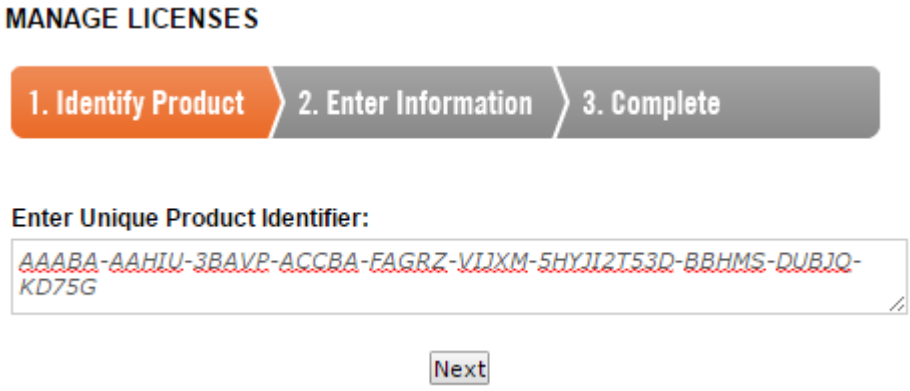
1. In the AppResponse 11 web UI go to Administration > Other: Licensing.
2. Enter the Product Key.
3. Enter the Email address of the user activating the license.



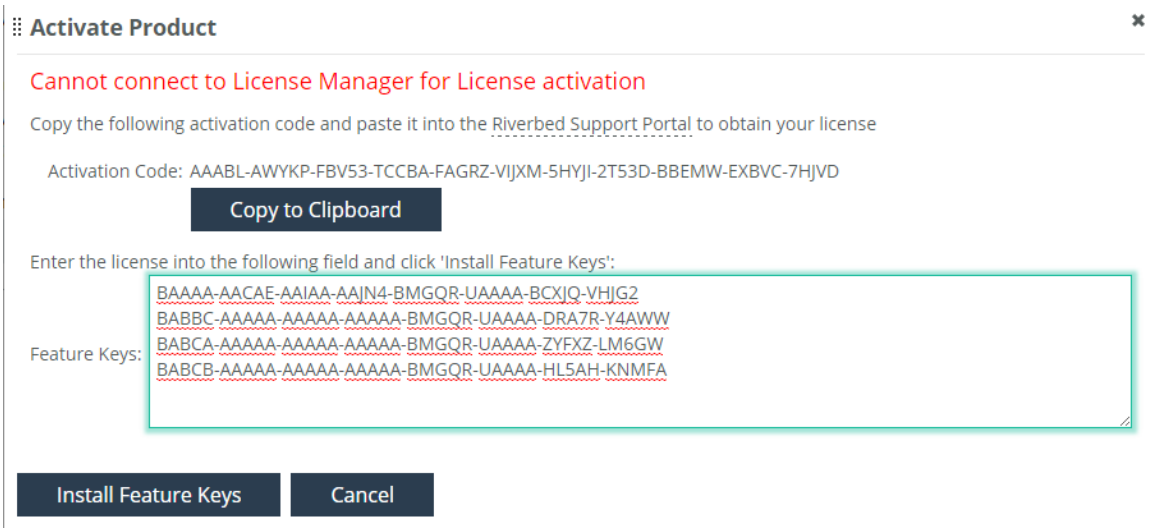
4. Click **Activate Product**. The Activate Product window opens.



5. Click **Copy to Clipboard.** The Activation Code is used to access the Feature Keys on the Riverbed Licensing site.
6. On a computer with an Internet connection, go to the Licenses page of the Riverbed Licensing web site (https://licensing.riverbed.com) and paste the Activation Code in the Enter Unique Product Identifier box.



7. Click **Next**. The Product Key is activated and the Product Key Details are displayed. The License Status is assigned and the Available Feature Set table shows each license Feature Key.
8. Return to the Activate Product screen in the AppResponse web UI and copy the Feature Keys, one per line, in the Features Keys text box. *The first key must be the CLMF-FRAMEWORK feature key.*



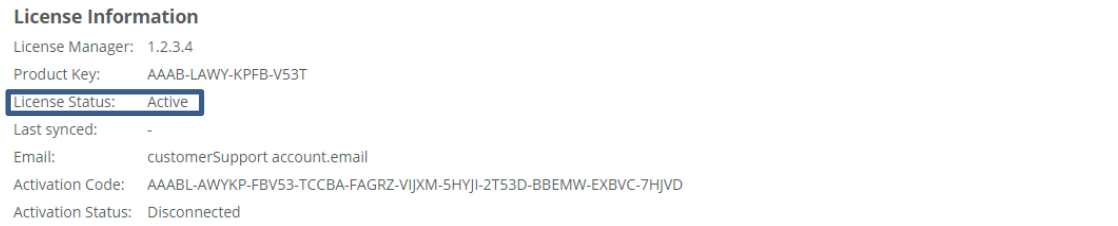
9. Click **Install Feature Keys** to finish the installation**.**

Deactivating an Active Virtual Edition License

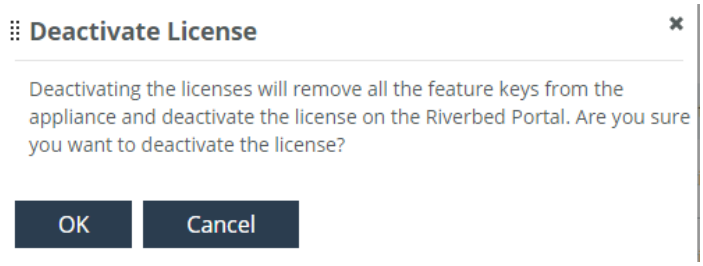
An AppResponse 11 virtual edition license can be deactivated and used again on an AppResponse 11 virtual edition. When deactivating a license:

- Only a license with an Active License Status on the License Information page can be deactivated.
- Copy the Deactivation Code that is displayed during the process on the web UI page. This code is used to deactivate the license and allow reactivation.
- You must delete the existing license *after successfully deactivating the license*.

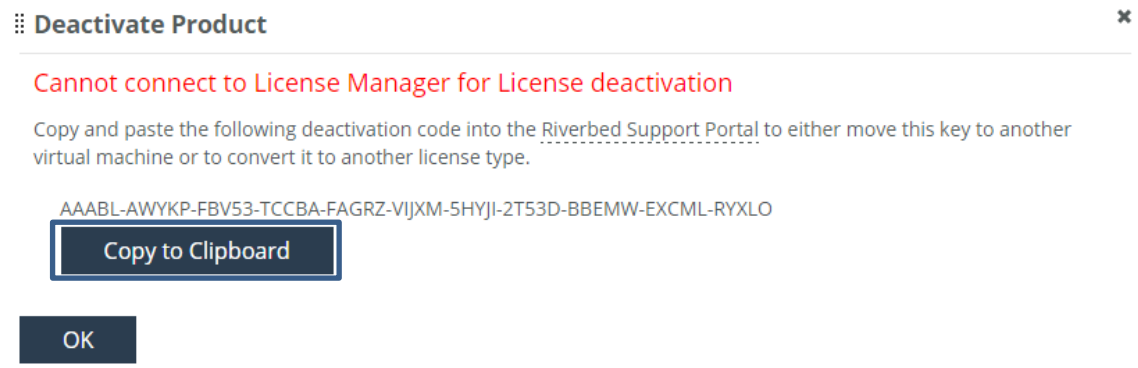
1. In the AppResponse 11 web UI go to Administration > Other: Licensing.
2. On the License Information page, confirm that that the License Status is Active.



3. In the toolbar over the Feature keys table, click **Deactivate**.
4. The Deactivate License window opens and asks for deactivation confirmation. Click **OK**.



5. The Deactivate Product screen appears (the License Information page with a Delete License button may appear first; ignore it for the moment). The Deactivate Product screen displays a deactivation code, used on the Riverbed Licensing site to deactivate the license and allow reactivation.



6. Click **Copy to Clipboard** to save the deactivation key.
7. Click **OK**.
8. Inform the license provider that the Product Key was deactivated. When completed, the Product Key is again available for installing AppResponse 11 virtual edition.

   - If the AppResponse 11 virtual edition has an Internet connection, the license deactivation occurs automatically.

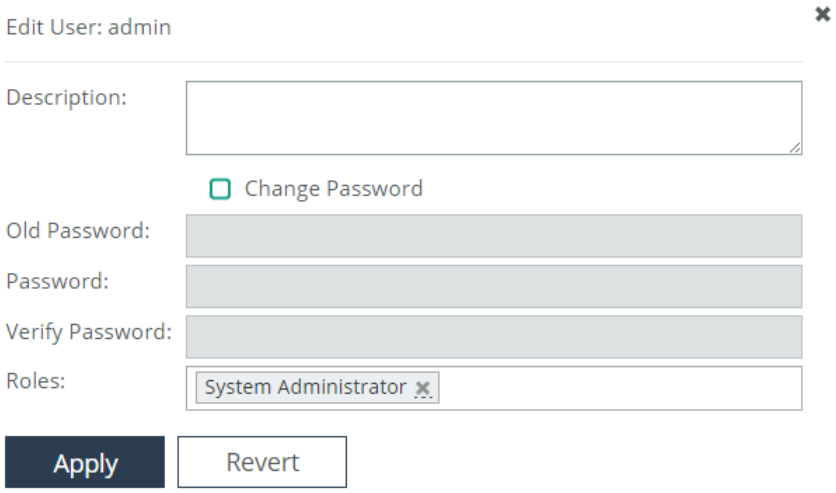
   or

   - If there is no Internet connection, go to the Riverbed Licensing site and paste the deactivation key in the Enter Unique Product Identifier box under Manage Licenses.
9. Click **Delete License**.

Changing the default password

When installation is finished, you can change the default password using the AppResponse 11 web user interface.

1. Go to Administration > Authentication: User Administration.
2. Select the admin user in the table.
3. Click the pencil (edit) icon that pops up at the end of the row.
4. Check the Change Password box.
5. Enter the old password and the new password.
6. Click **Apply** when finished or **Revert** to cancel the change.
7. Record your new password in a safe place.
   Note: If lost, this password cannot be recovered by Riverbed.



Additional configuration

To complete the configuration of AppResponse 11 for traffic monitoring, including setting up interfaces, capture jobs, groups and policies, refer to the *SteelCentral AppResponse 11 User's Guide* or the online Help available from the AppResponse menu bar.

Beyond the basics

Adding a monitor port

You can have up to four monitor ports in AppResponse 11 virtual edition. The first monitor port is configured as part of the initial deployment of AppResponse 11. You can configure additional monitor ports after the initial deployment by following the procedure given below.

In most cases you would not put multiple monitor ports on the same virtual switch; thus, the first step in the procedure is to create a new virtual switch. You might, however, make an exception to this practice if the ports were part of port groups on separate VLANS.

In general, though, the procedure for adding a monitor port would contain these steps:

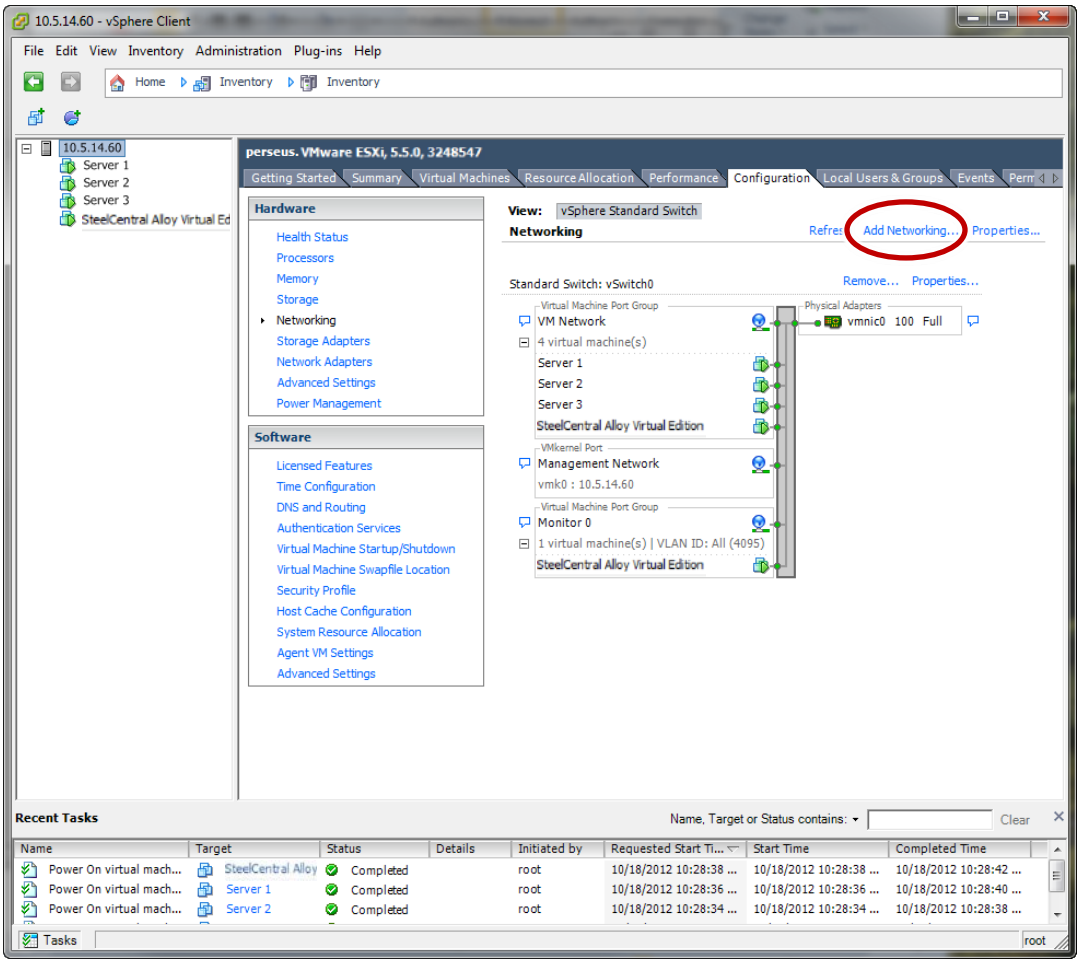
- create a new virtual switch and port group
- set the new port group to promiscuous mode

- create a new monitor port in the new port group
- reboot AppResponse 11 to see the port added to the monitoring interfaces

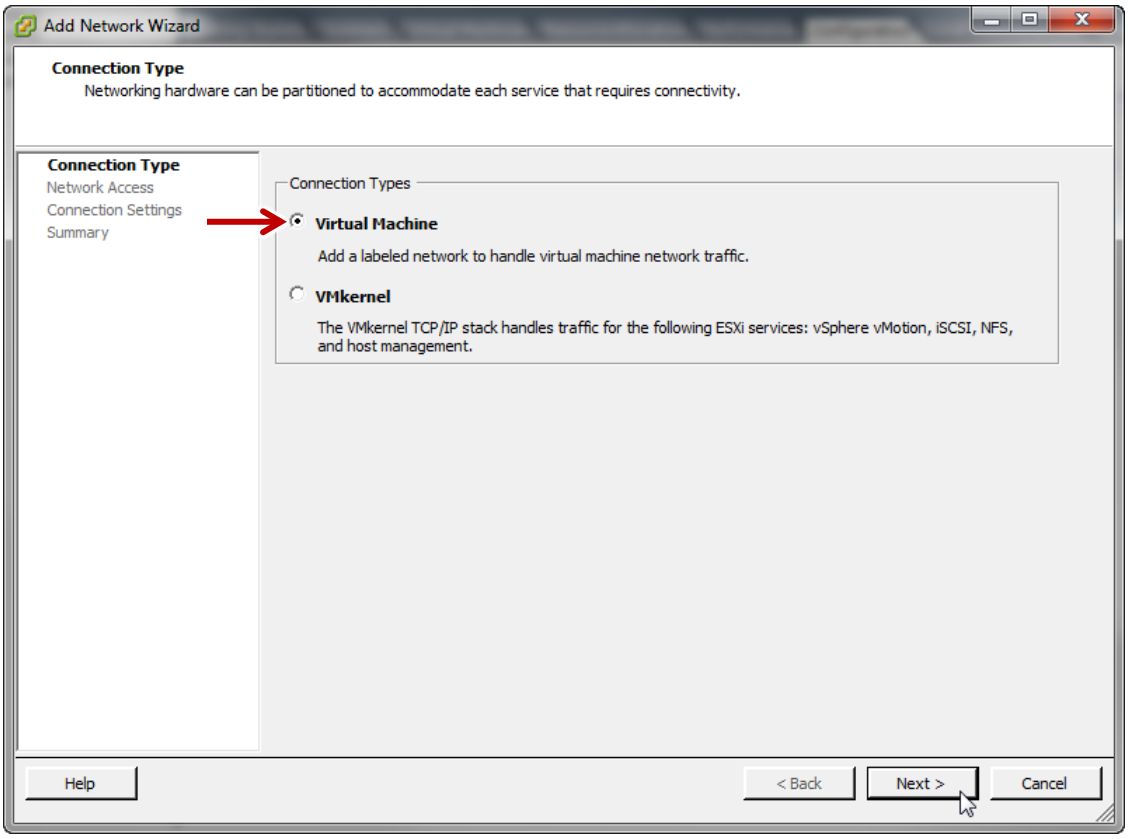
The rest of this section provides the detailed procedure.

Create a new virtual switch and port group

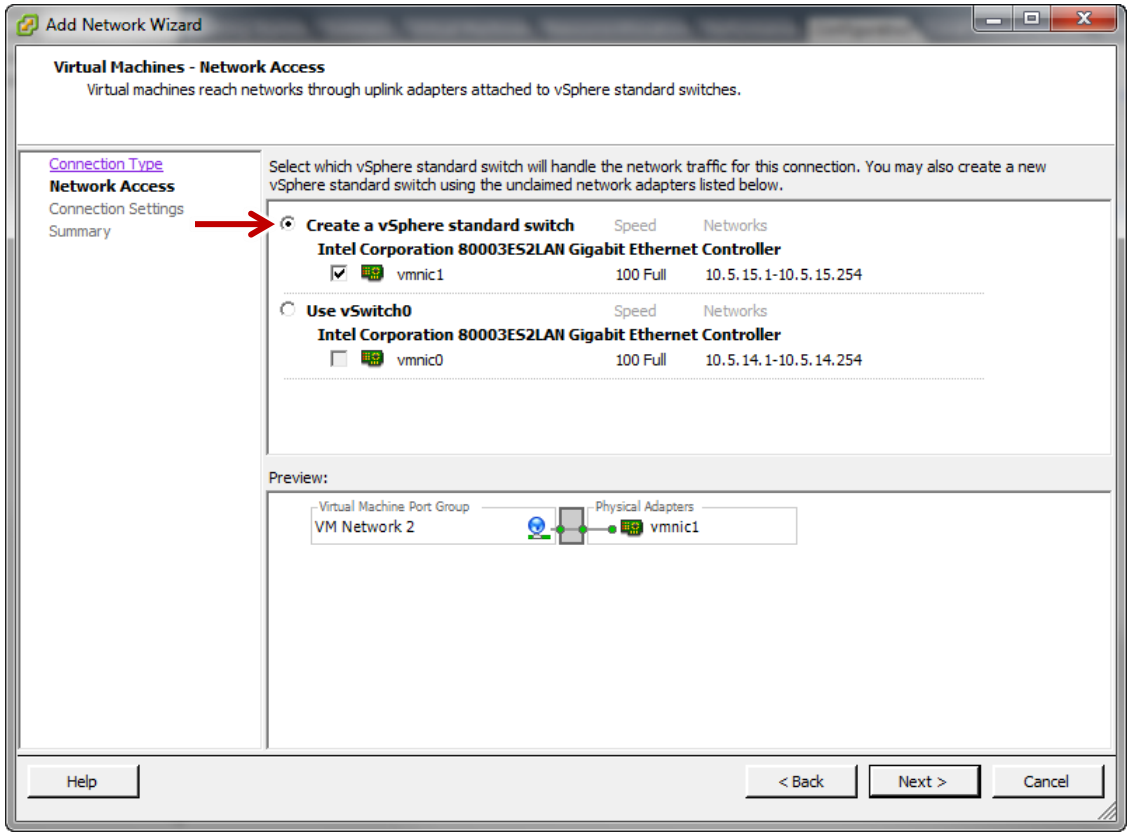
1. On the ESXi server's networking configuration page, click ***Add Networking…***.



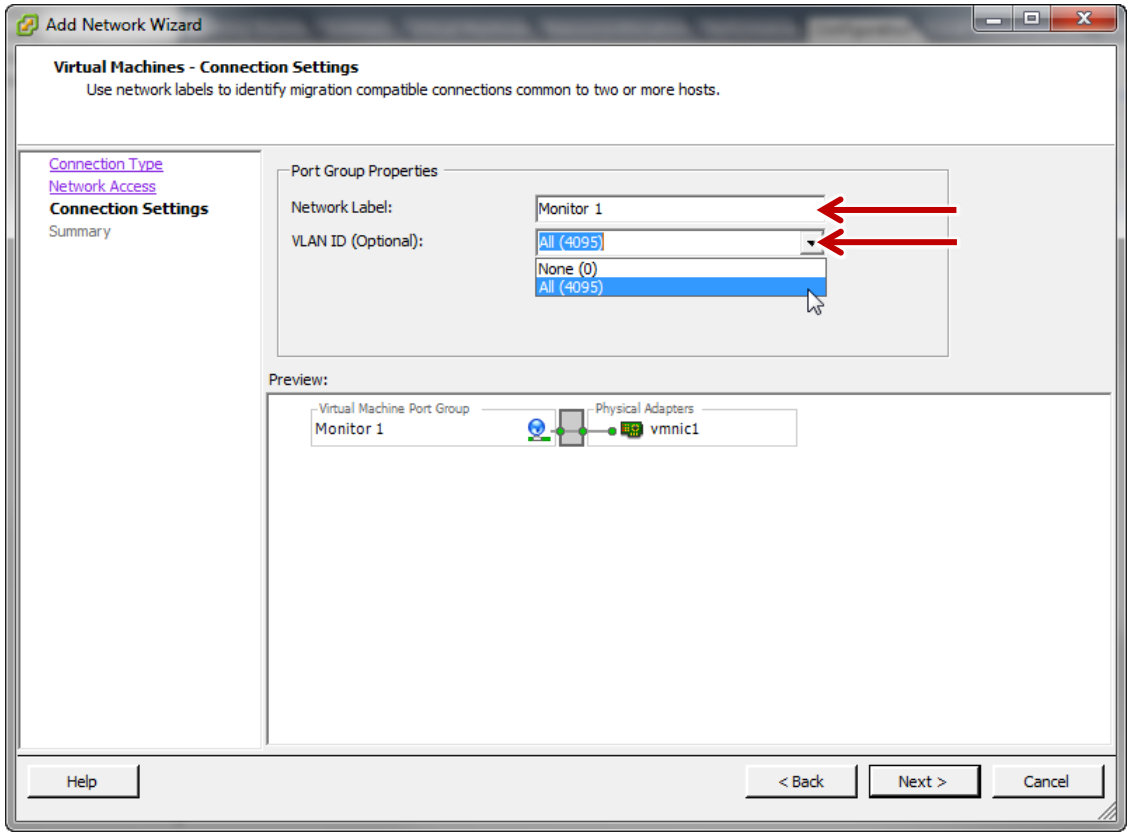
2. Select ***Virtual Machine*** as the connection type.



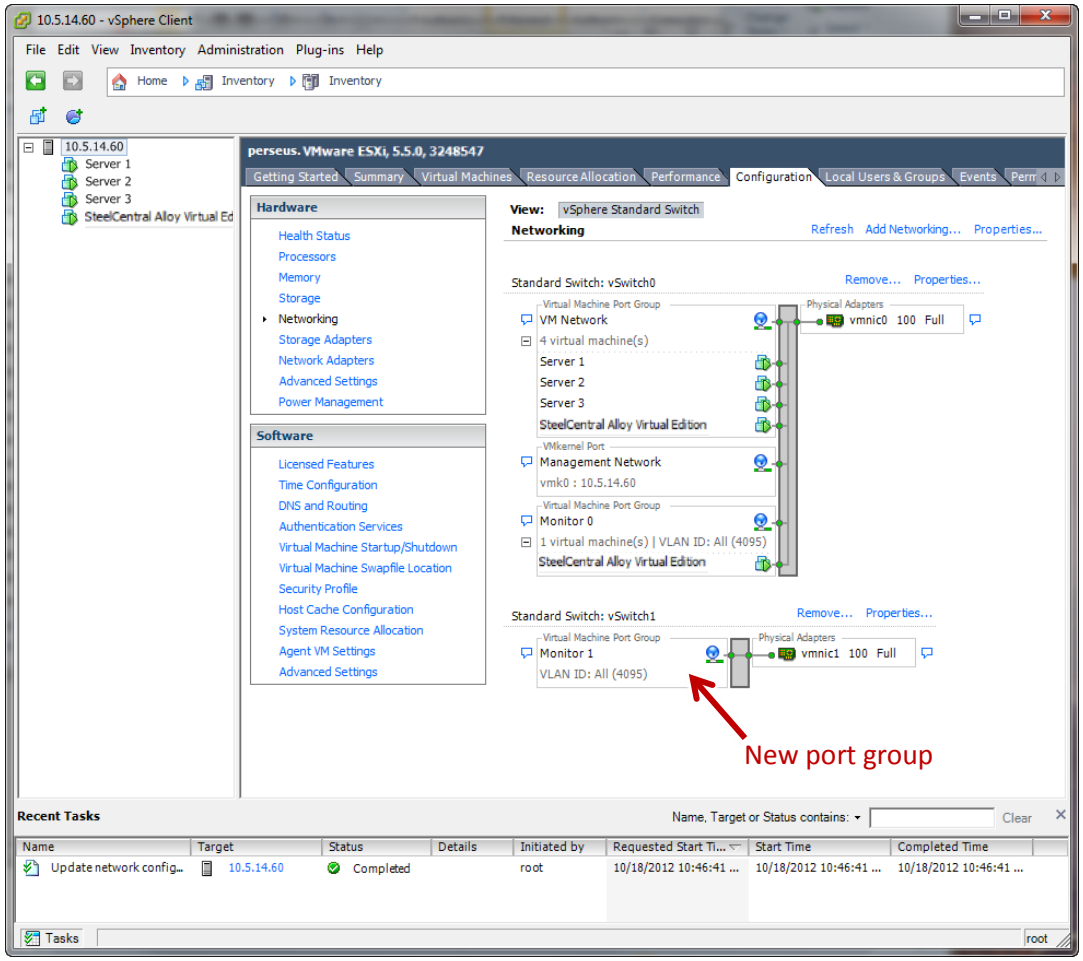
3. Select ***Create a vSphere standard switch***. The ***Preview*** pane at the bottom of the screen shows what the arrangement of port groups on the switch will be.



4. Enter a name for the port group in the ***Network Label*** field. Select a ***VLAN ID*** of ***All (4095)***. This will allow the port group to see all tagged and untagged traffic on the switch.



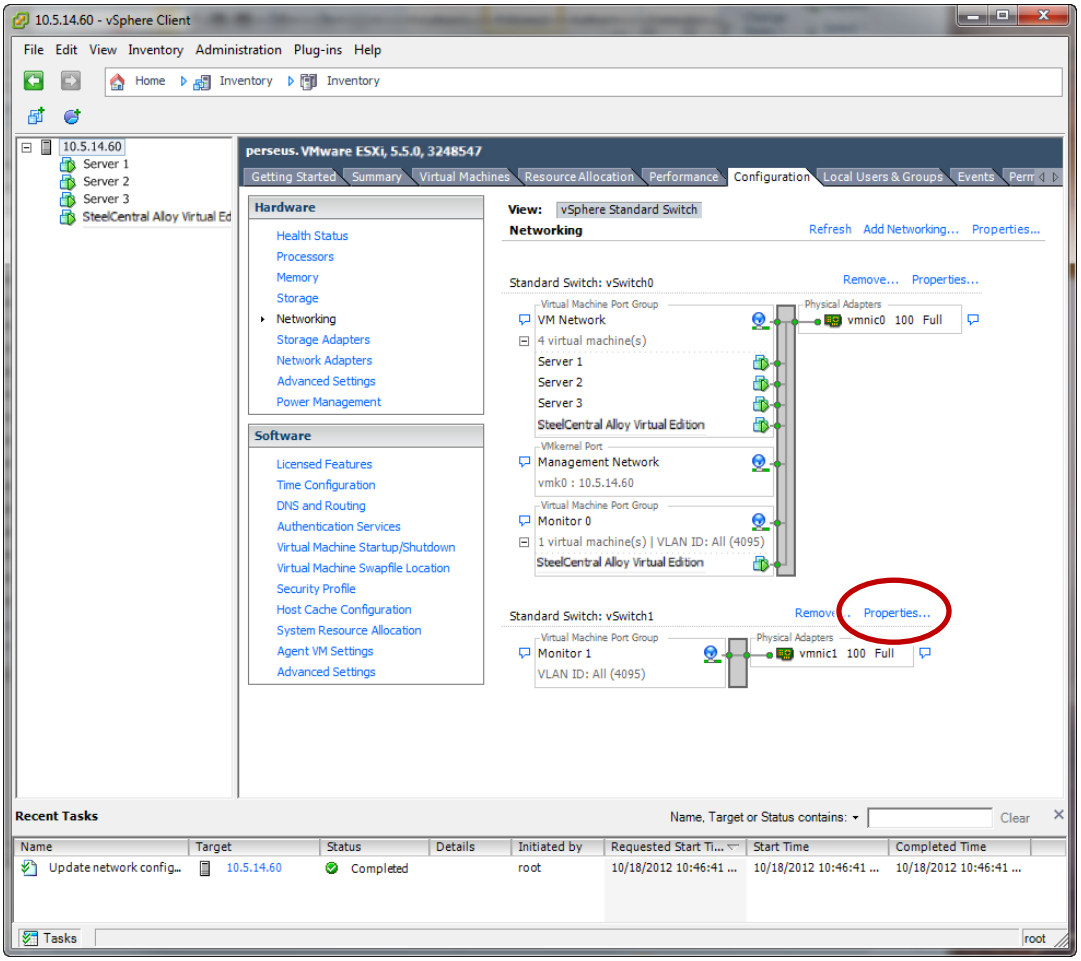
5. On the ***Ready to Complete*** page click ***Finish***. The new port group will be configured on vSwitch1 and the configuration will look like this:



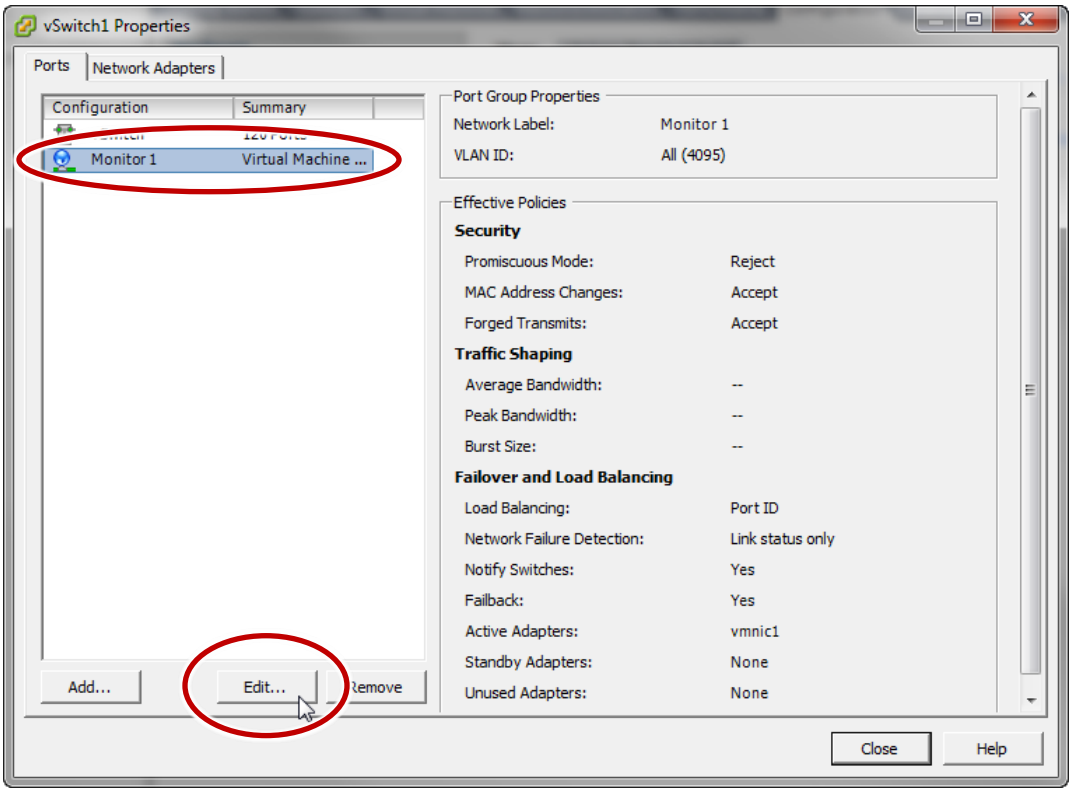
Set the new port group to promiscuous mode

Set the new port group, Monitor1, to promiscuous mode.

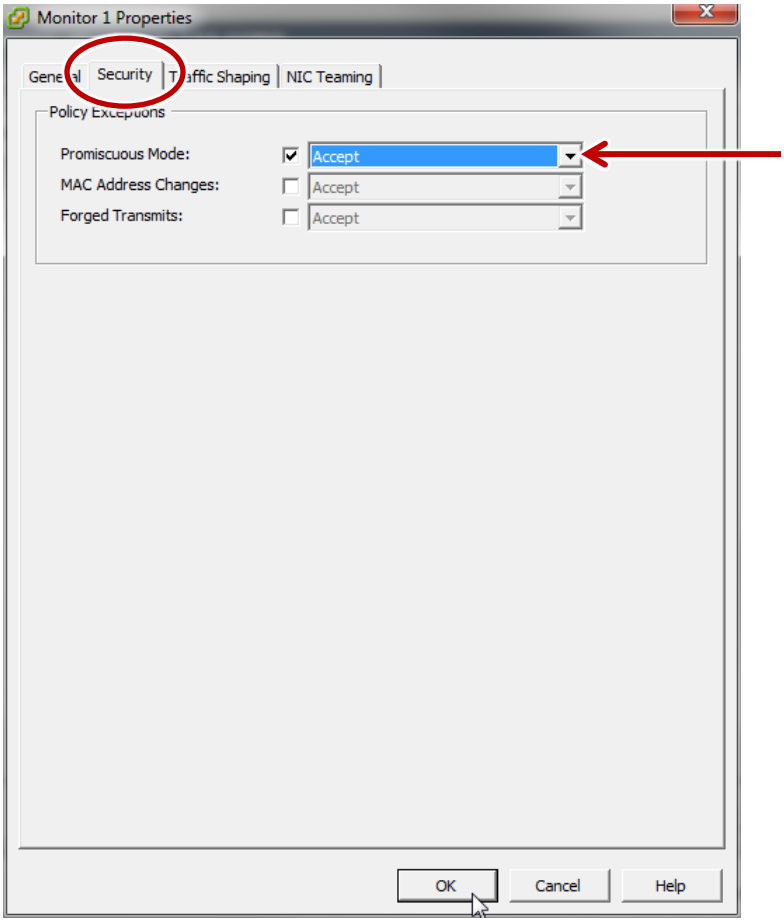
1. In the networking configuration page, click the ***Properties...*** link for vSwitch1.



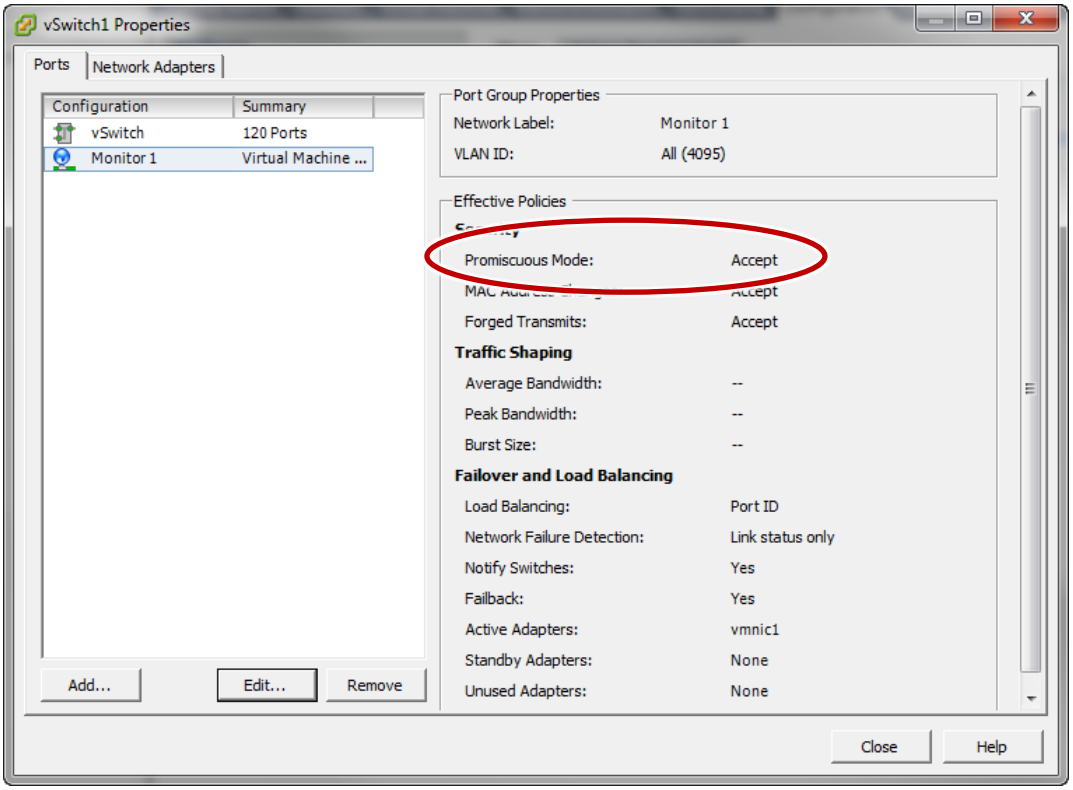
2. Select the ***Monitor1***port group and click the ***Edit...*** button.



3. Click the ***Security*** tab, check the ***Promiscuous Mode*** check box, and select a value of ***Accept***. Click ***OK***.

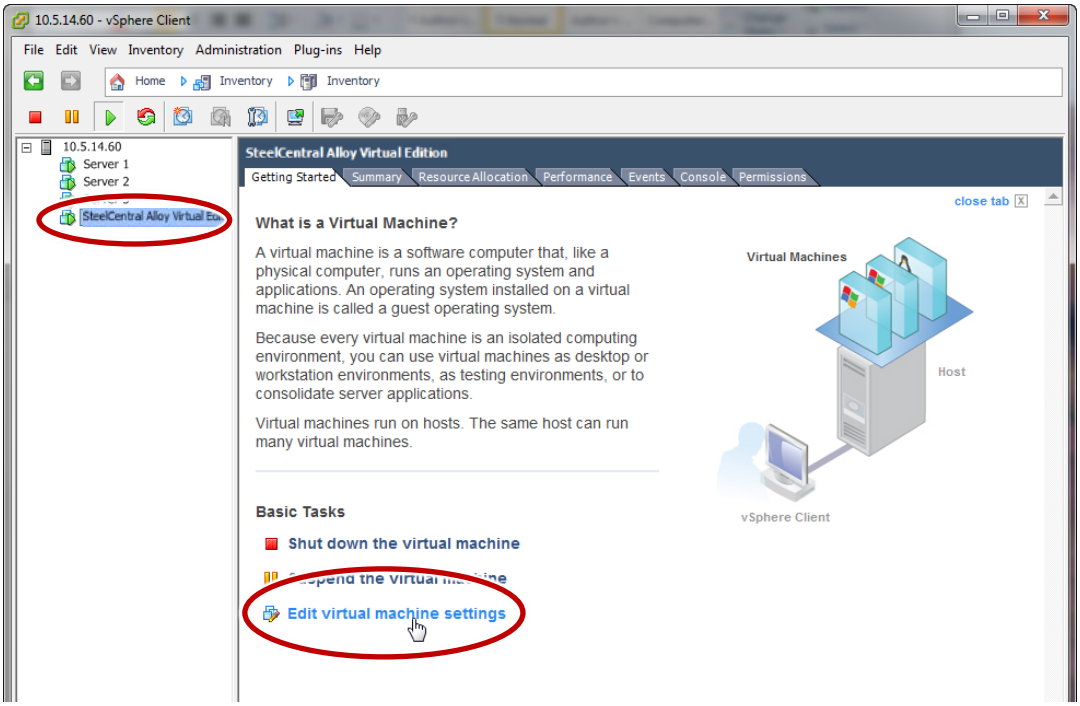


4. Verify that ***Promiscuous Mode*** for the Monitor1 port group is set to ***Accept***. Then click ***Close***.

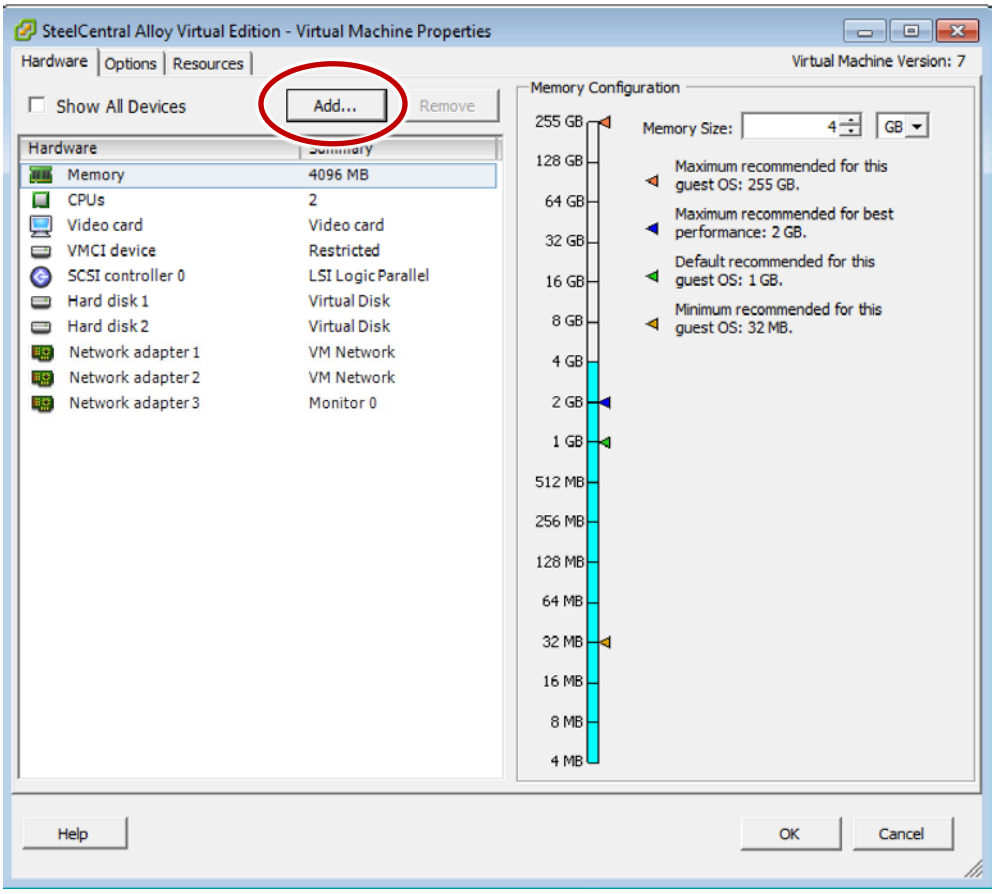


Create a new monitor port in the new port group

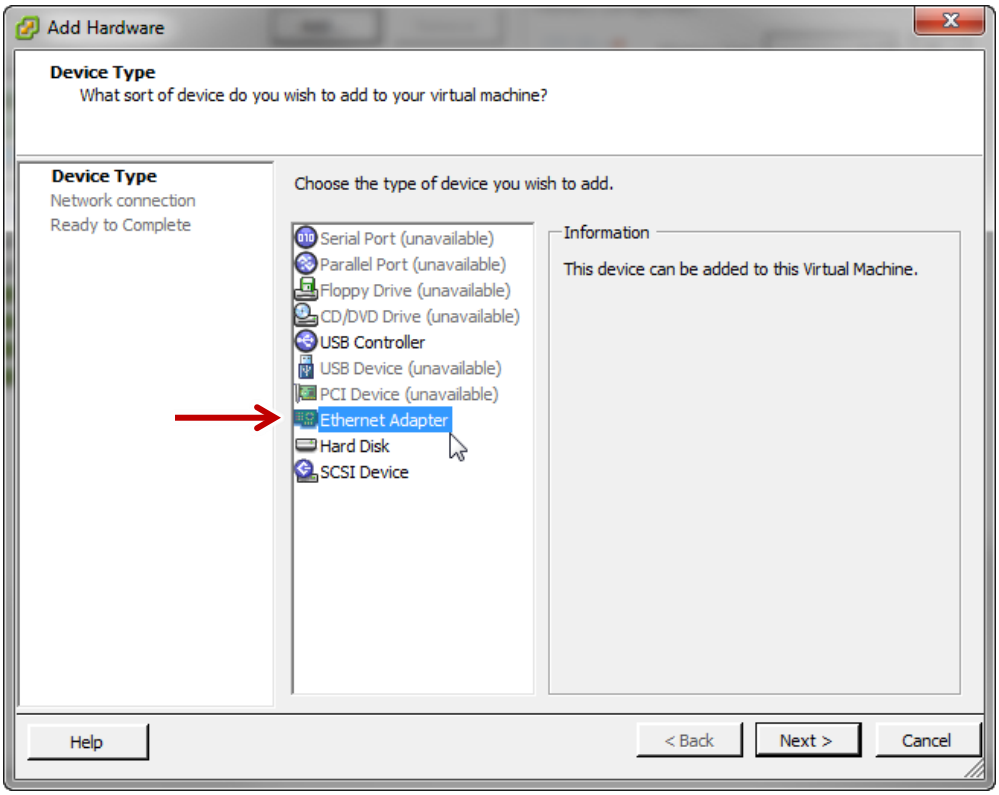
1. Select the AppResponse 11 and click ***Edit virtual machine settings***.



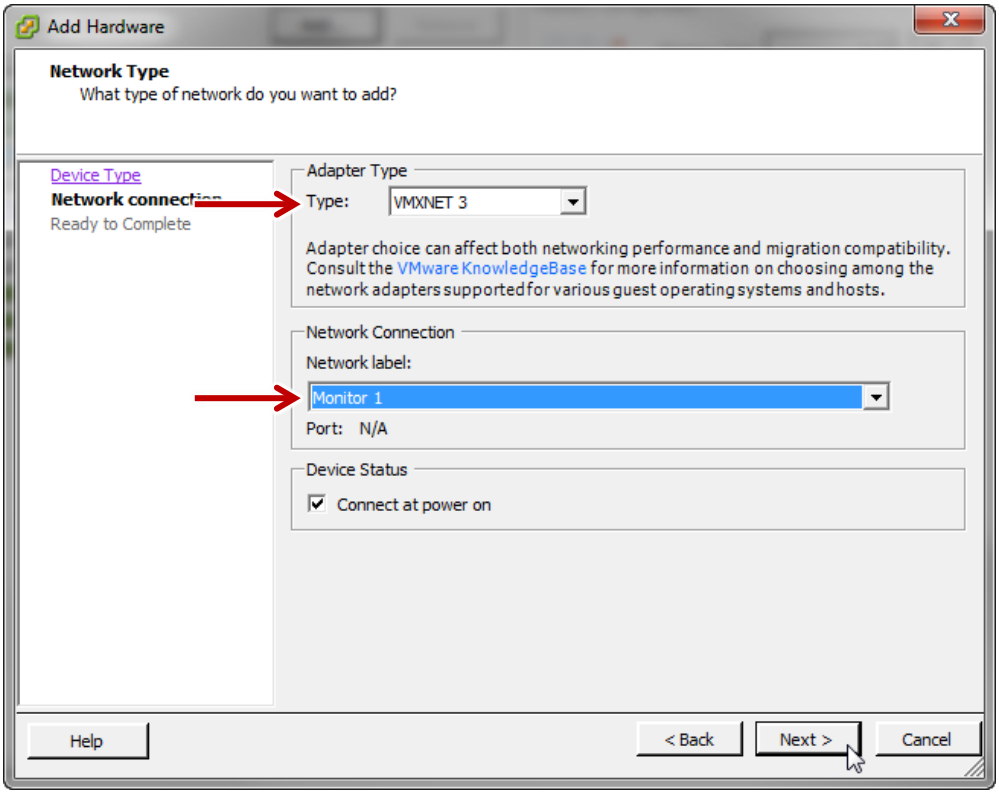
2. On the ***Virtual Machine Properties*** page, click ***Add...***.



3. On the ***Device Type*** page, select ***Ethernet Adapter***.



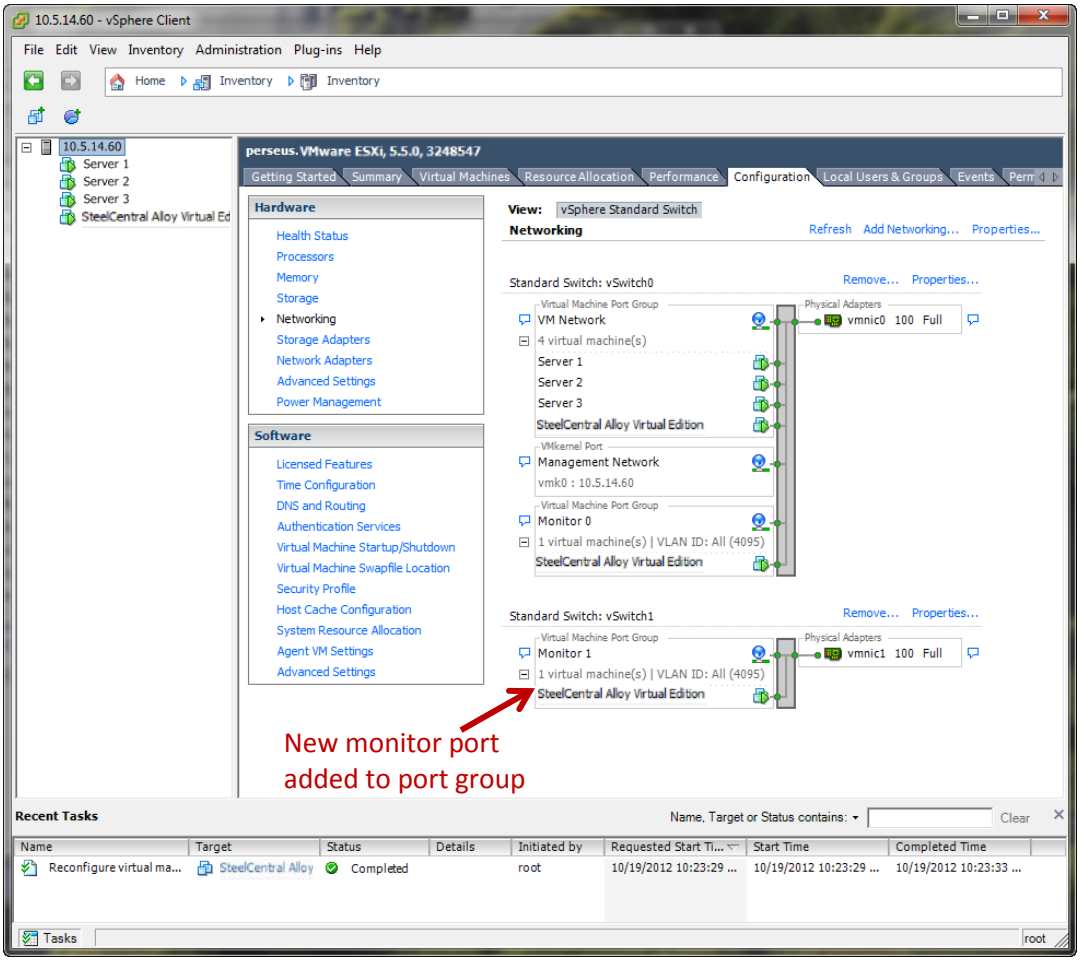
4. On the ***Network Type*** page select ***VMXNET3*** for the ***Adapter Type*** and for the ***Network Label*** select the name of the port group that you want to map the new monitor port to (***Monitor 1***).



5. On the ***Ready to Complete*** page, click ***Finish*** to create the monitor port and add it to the port group.

6. The ***Virtual Machine Properties*** page shows the new monitor port ready to be added. Click ***OK*** to add it.

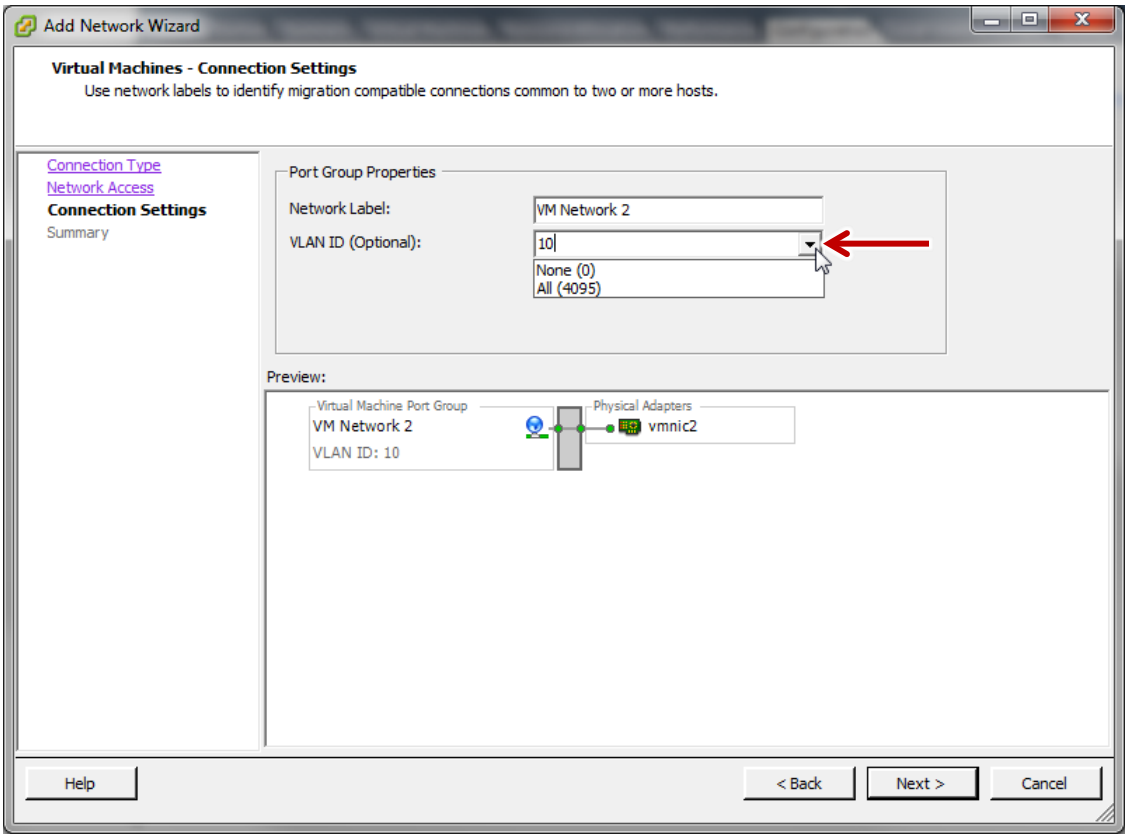
The ***Networking*** view on the ***Configuration*** tab of the server shows the AppResponse 11 added to the Monitor 1 port group, indicating the mapping of the new monitor port (***mon1***).



Important: Make certain to reboot the AppResponse 11 so that the new interface will be visible in the Web UI's Monitoring Interfaces page.

VLANs

When you are setting up a port group, the ***Virtual Machines – Connection Settings*** screen allows you to specify a ***VLAN ID***. You can select ***None (0)*** or ***All (4095)*** from the drop-down list, or you can enter a single VLAN ID in the text box.



The effect of the ***VLAN ID*** entry is:

If you enter:	**Devices attached to this port group will be able to see these packets on the virtual switch:**
None (0)	untagged packets
All (4095)	untagged packets plus packets tagged for all VLANs
a single numeric VLAN ID (for example, 10)	packets tagged for the specified VLAN

Note that if the port group is set to non-promiscuous mode, a device in the port group will be able to see only packets that are addressed to it. If the port group is set to promiscuous mode, a device in the port group will be able to see packets with any destination address.

NFS datastores and thick provisioning

The ESXi server supports local, NFS, and iSCSI datastores.

By default, NFS datastores use thin provisioning regardless of whether you have specified thin provisioning or thick provisioning when deploying the OVA or adding a hard drive. You can, however, force a hard drive stored on an NFS datastore to use thick provisioning in the following way:

1. If the AppResponse 11 is powered on, power it off.
2. Go to the ***Configuration*** tab of your ESXi server.
3. Click ***Storage***.
4. Right-click the datastore where your virtual hard disk is located and choose ***Browse datastore***.
5. Click the Folders tab, and then select the folder corresponding to the virtual machine of interest.
6. Right-click on the virtual hard disk of interest and select ***Inflate***.

The ESXi server will physically reserve the configured amount of storage. Note that depending on the size of the virtual hard disk and the connection speed, inflation can take a long time, possibly hours.

Optional customizable storage

For many models of AppResponse 11 appliance, you have the option of configuring the system with reduced packet storage space in order to store more analysis data. Two modes are supported:

- Packet data priority mode (pktprio) is the default, and is similar to the configuration of the earlier Shark platform, maximizing packet storage and using a smaller retention time for other data.
- Metric priority mode (metprio) is similar to the configuration of the earlier AppResponse 9 platform, increasing the retention time of analysis modules including aggregates, probe, WTA, DB performance and VoIP, but reducing the packet storage accordingly. On the ARX-6000, metprio mode does not allow selection of a storage unit (EXP-300).

The AppResponse 11 appliances that support these modes are:

- ARX-3300
- ARX-3800
- ARX-4300
- ARX-5100
- ARX-6000
- SCAN-02170
- SCAN-04170
- SCAN-06170
- SCAN-08170
- VSCAN-0100
- VSCAN-0500
- VSCAN-2000

In each mode, the general behavior of the system is the same, but the location where packet and analysis data is stored changes, and the amount of space allocated for each type of analysis data and for packet data varies. If you have a lot of existing analysis data, the transition from pktprio to metprio could take a long time. The layout configuration process should preserve all analysis data, except that packet capture data on the destination data section will be lost.

Note: The transition of storage mode from pktprio to metprio is one-way and irreversible.

Note: Changing the RAID mode of a Storage Unit must be done prior to applying "metprio" mode. Before making any changes to the storage mode, you should evaluate any changes you may wish to make to the default RAID 0 setup on your packet storage units. Any RAID changes must be made before changing the storage mode. If you happen to do this in reverse order, you will need to perform a reinstall or do a factory reset from the web UI.

Note: For SCAN-06170 appliances, if a RAID6 48TB Storage Unit is selected as the metprio mode destination, packet_capture will not be used on that Storage Unit, and a second Storage Unit must be available in order to capture packets.

Note: For SCAN-08170 appliances, RAID6 48TB Storage Units are not valid selections for metprio mode. Any other Storage Unit in any other valid mode is usable.

Note: During the time the change from pktprio to metprio is in progress, you may see error messages displayed in the Web UI as a result of some background services stopping.

The configuration process is invoked via a CLI command, takes up to a few hours to run, and is followed by a mandatory reboot. After the reboot, various analysis components use the packet capture volume to store data, increasing their retention times. It is not possible to switch back to the original (default) mode. In order to change the storage mode (or to specify a different storage unit for metprio mode), either a factory reset or a full reinstallation is required, and the storage that was configured previously for metprio mode must be reinitialized.

VM deployments require a secondary disk in order to use packet capture or switch to metprio mode. The recommended sizes for the secondary disk are:

- VSCAN-0100: 100GB
- VSCAN-0500: 2TB
- VSCAN-2000: 8TB

If the secondary disk is not large enough, then any attempt to switch to metprio mode via the CLI will result in an error. If the secondary disk is too large, then the extra space will be unused.

Supported CLI commands

The following CLI commands are provided to support this feature:

- show storage layout: Display information about the current mode and the status of any operations.
- show storage layouts: Display a list of all available modes and valid data sections.
- storage layout metprio [data_section <data section>]: Change the storage layout mode to metprio.

Changing the storage mode

To change from packet data priority mode (pktprio) to metric priority mode (metprio):

1. Log in to the CLI as admin.
2. Execute: “enable”.

3. Execute: “configure terminal”.
4. Execute: “show storage layout” and verify that the current layout is “pktprio”.
5. Execute: “show storage layouts” and verify that the “metprio” layout is available with a valid data section. The valid data section should be:
   - “primary_capture_data” for non-SU systems
   - storage device name(s) for SU systems (e.g., LD8XU001934F5)
   - blank for ARX-6000 systems
1. Execute the command to reconfigure the storage layout.
   - For non-SU systems: “storage layout metprio data_section primary_capture_data”
   - For SU systems: “storage layout metprio data_section <storage_device_name>”
   - For ARX-6000s: “storage layout metprio”
7. Respond “yes” to the prompt to initiate the layout reconfiguration.
8. The layout reconfiguration progress is reported on the CLI:
   “Reconfiguring to layout 'metprio' ... xx% ... yy%.”
   The duration of the layout reconfiguration depends upon the amount of analysis data that needs to be transferred. The layout reconfiguration is complete when the final status that is reported on the CLI shows “Done” and you are prompted to reboot on the CLI and the Web UI.
9. Respond “yes” to the CLI reboot prompt or reboot from the Web UI.
10. After the reboot, the system is in metric priority mode. You can confirm this by executing “show storage layout” in the CLI. The current layout now should be “metprio”.

Contacting Riverbed

Options for contacting Riverbed include:

- Internet - Find out about Riverbed products at http://www.riverbed.com.
- Support - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Technical Support or your channel partner who provides support. To contact Riverbed Technical Support, please open a trouble ticket at https://support.riverbed.com or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.
- Professional Services - Riverbed has a staff of engineers who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom-coded solutions. To contact Riverbed Professional Services, go to http://www.riverbed.com or email proserve@riverbed.com.
- Documentation - Riverbed continually strives to improve the quality and usability of its documentation. We appreciate any suggestions you may have about our on line documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com