Appliance Enterprise Deployment Guide

Published: July 2012
Updated: August 2013

Applies To

API Gateway v6 and v7

Feedback

Send suggestions and comments about this document to support@axway.com

Introduction

After the initial install of the Appliance software there are a number of default settings which the user should be aware of. This document outlines those settings and provides instructions on how each setting can be modified to the users needs.

Web Administration Interface (WAI)

Most of the modifications can be carried out using the Web Administration Interface (WAI). This can be accessed by pointing a web browser at:

```
https://<server>:10000
```

where <server> can be the IP address or hostname of your server. So for example, if your server IP address is 192.168.0.100 then you would be able to access the WAI for that server at:

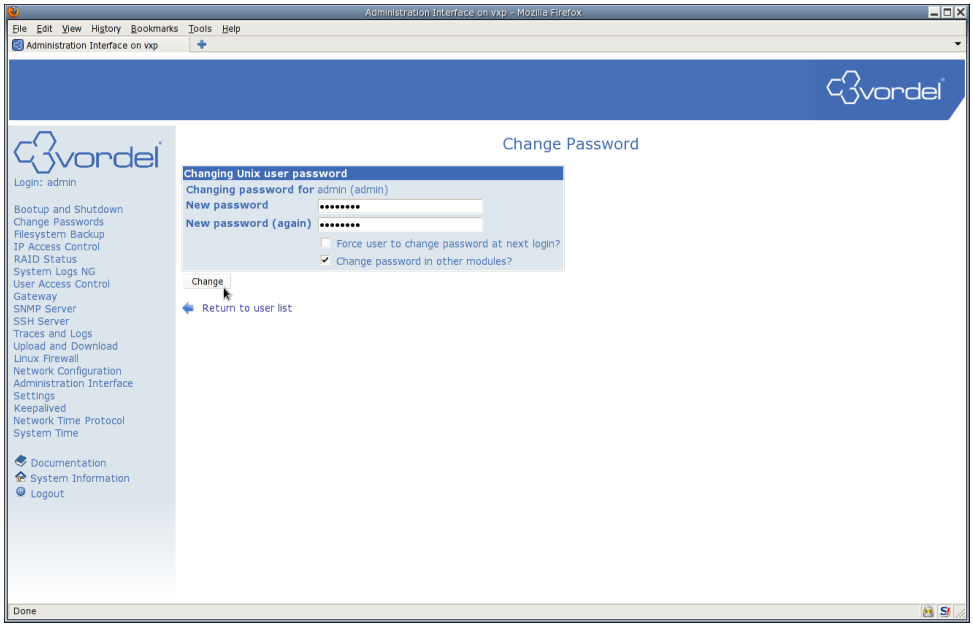
```
https://192.168.0.100:10000
```

The default access to the WAI is possible using the `admin` user and the password `changeme`.

The connection to the WAI is over HTTPS but the certificate is self signed, and as such will trigger an untrusted connection message when connecting from most major web browsers. This is nothing to be alarmed about, it just indicates that the certificate is not in the web browsers trusted store. You have the option of adding this identity to the store to continue the connection.

OS and Software Versions

The Appliance base OS is a modified install of Oracle Linux 5.6. However, due to the fact that the Appliance tracks security updates to packages there are a number of more recent builds of certain software on the system. Notably, the kernel installed is currently the “Oracle Unbreakable Kernel” 2.6.32-200.23.1.el5uek.



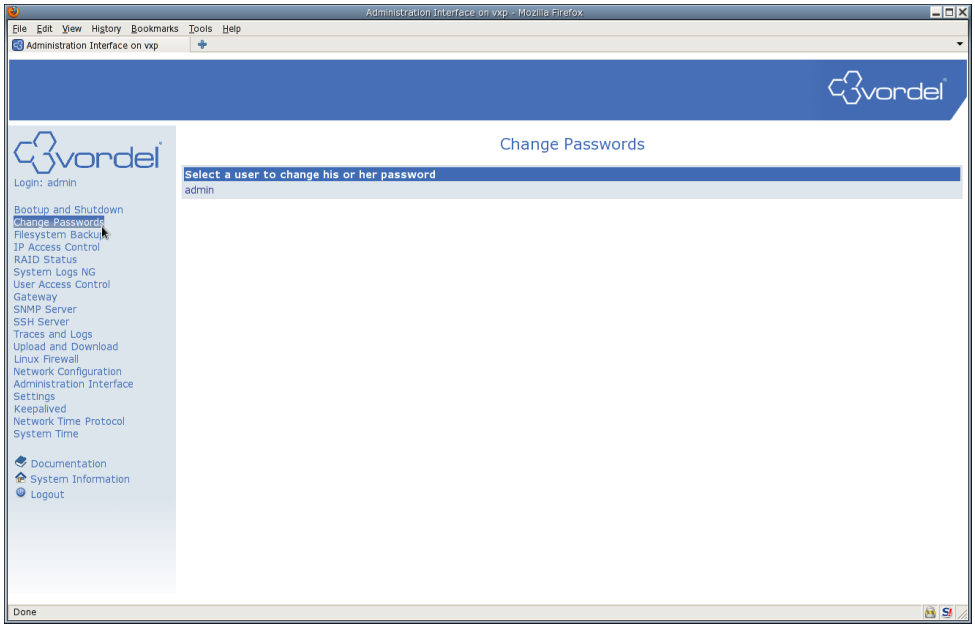
Modifying default passwords

The system ships with a default password to ease initial administration and configuration. It is *highly recommended* that the user change the default password immediately to avoid security issues with their system. Also, the initial default password for the `root` and `admin` user are identical. In a live system it is recommended that these password do not match.

admin

The admin password can be changed a number of ways. The easiest is by using the WAI.

Log in to the WAI and select Change Passwords from the menu on the left.



Select the admin user, enter the new password in the text boxes, and click the change button.

root

The default root password in `changeme`. As root is an important user, it is not possible to change the password through WAI. To change the root password you must log in to the Appliance through ssh. As a security precaution, the root user is not able to log in to the Appliance through ssh directly. First you must log in as the admin user, the execute the command ‘su -’ to switch to the root user.

```
$ ssh admin@appliance
admin@perf's password: <enter-admin-password>
Last login: Thu Feb 16 10:26:12 2012 from 192.168.0.200
[admin@appliance ~]$ su -
Password:  <enter-root-password>
[root@appliance ~]
[11:44:14]#
```

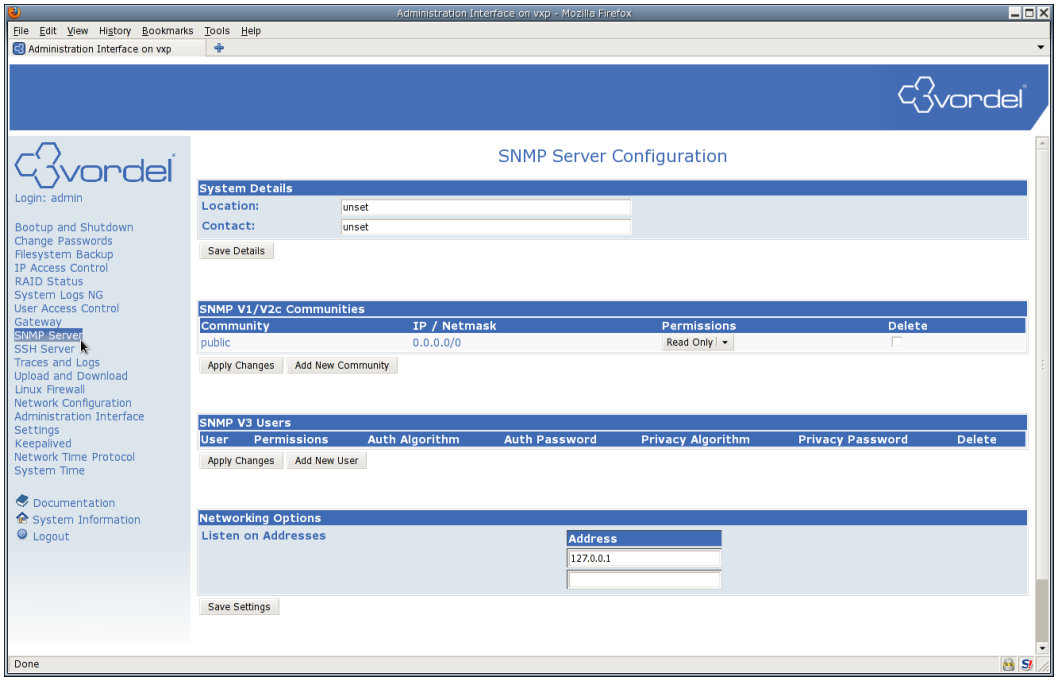
Enter the passwd command to change the root password.

```
[11:45:02]# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@appliance ~]
[11:45:07]#
```

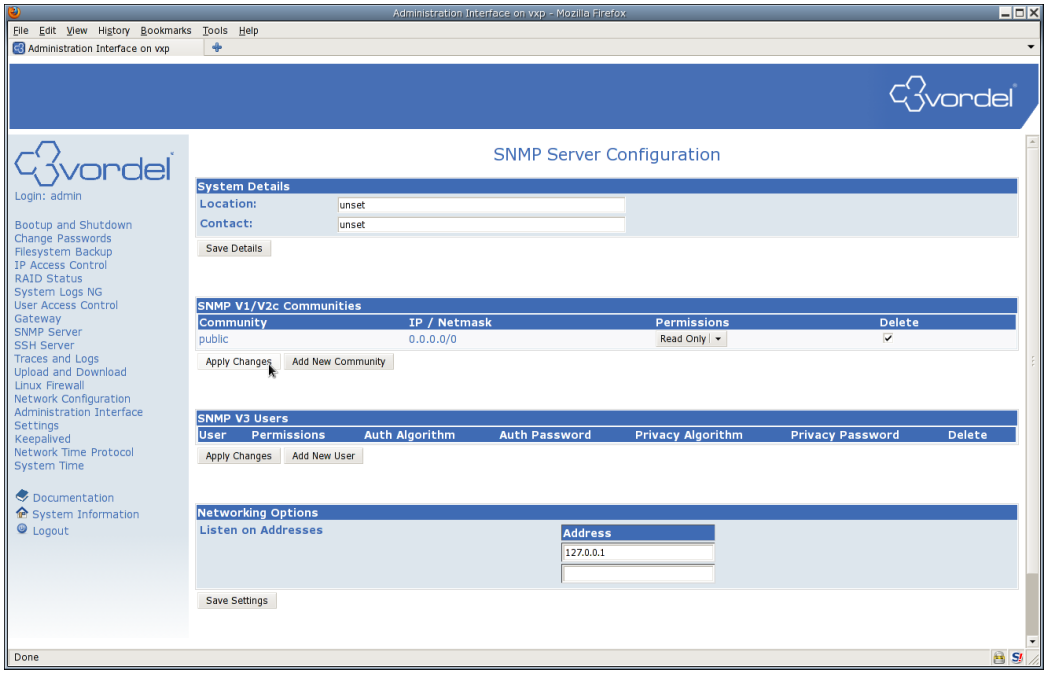
SNMP v1/v2c Community

The default SNMP community of public exists on the system. SNMP is disabled by default on the Appliance but if the service is enabled, the default community allows read only SNMP access to all IP addresses. To change this behaviour follow these steps:

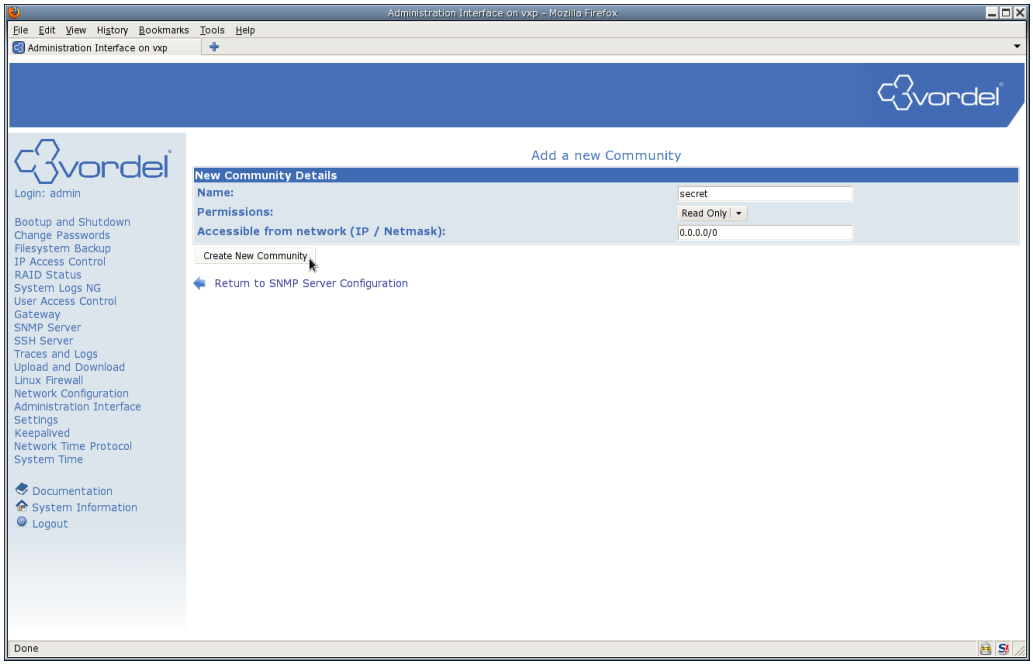
Log in to the WAI and select SNMP Server from the menu on the left.



Tick the checkbox to select the public community, and click the Apply Changes button



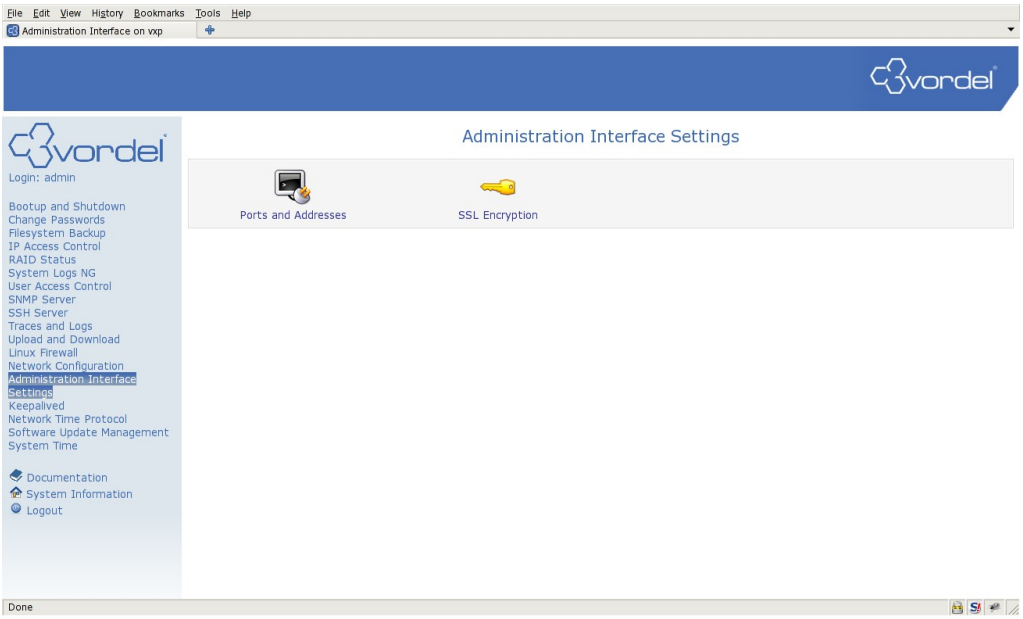
Click Add New Community and enter a new community name (secret in this example). Also enter an allowable network to connect from (unrestriced 0.0.0.0/0 in this example). Click the Create New Community button to save the changes.



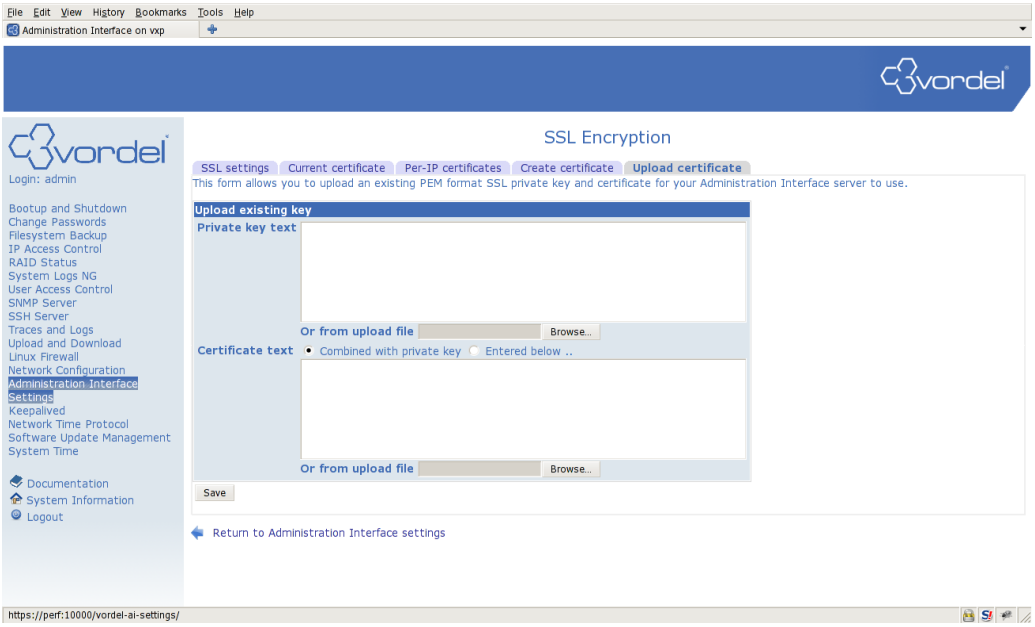
Modify Default WAI SSL Certificate

To upload a new SSL certificate to the Web Administration Interface follow these steps.

First log in to the WAI and select Administration Interface Settings



Then click SSL Encryption and select the Upload certificate tab. Either enter the text of your certificate or upload it from file and click the Save button.



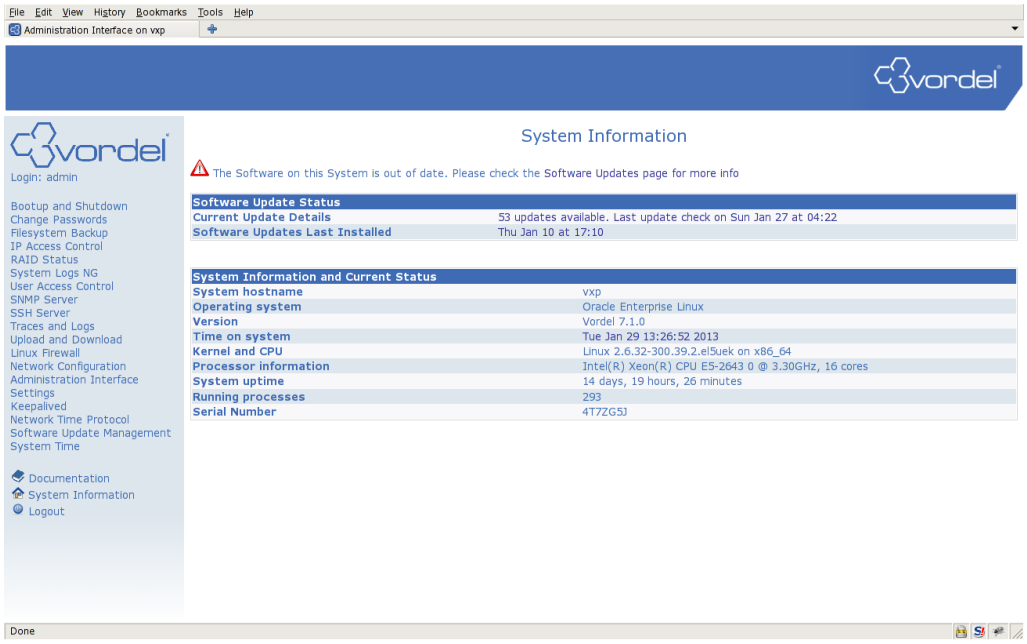
Keeping System Software Up to Date

The Appliance provides an automatic software update checking mechanism which can be accessed and modified through the WAI.

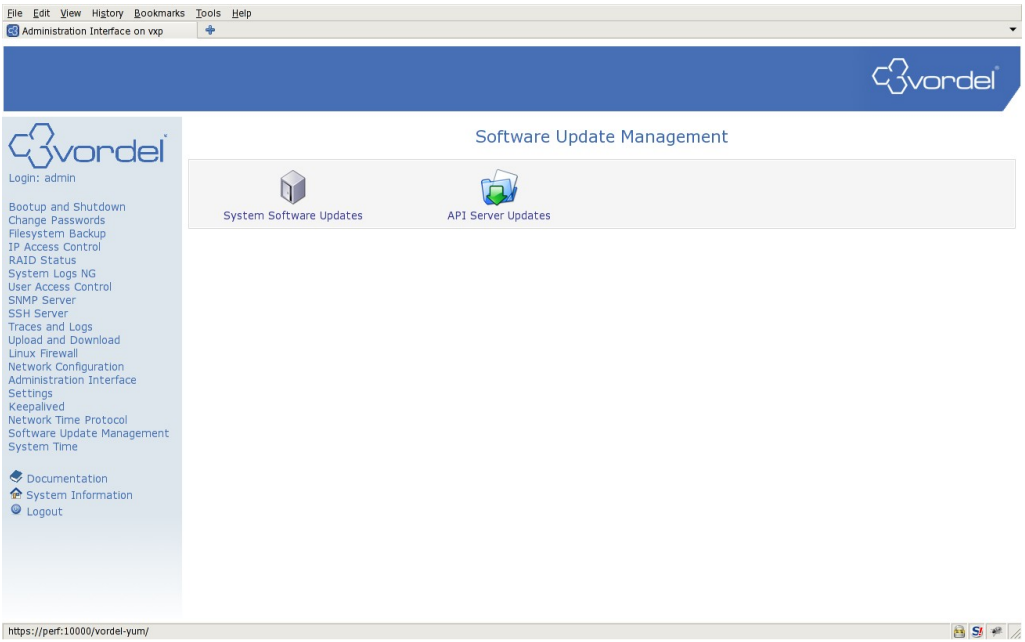
By default, the system scans a centralised software update repository once a week on a Sunday night. If updates are available they are listed on the WAI after the user logs in. It is recommended that this behaviour is modified to a schedule the user is comfortable with and that an email address is provided for email notification of software update availability.

Software Update Status Screens

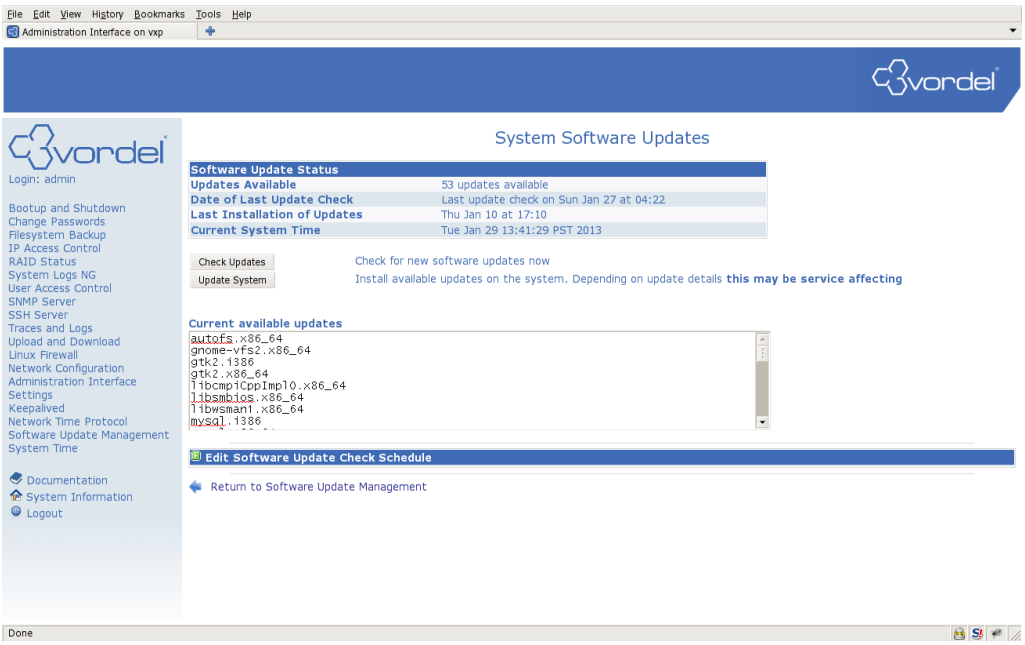
This is the System Information page which is presented when the user logs in. If software updates are available a warning is presented with some details on how many updates are available, the date/time of the last update check, and the date/time when the last updates were installed.



More details and configuration/update options can be found by clicking on the Software Update Management link on the left. Here the user can find links to the System Software updates and the API Gateway Software updates. It is not necessary to update the API Gateway Software to keep the system up to date with the latest OS and software patches.

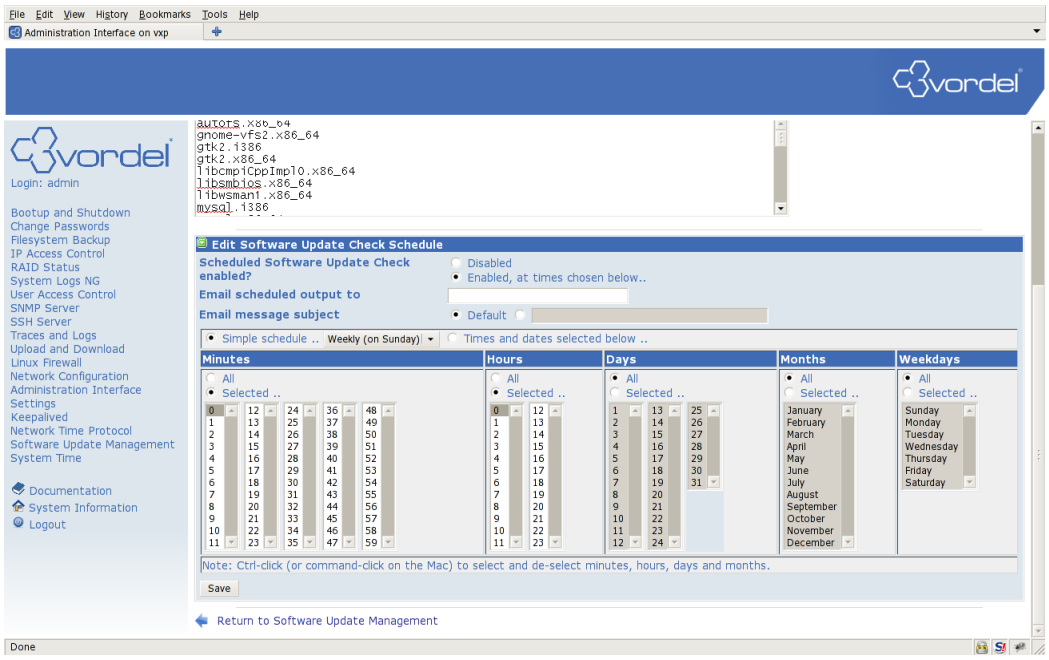


Clicking on the System Software Updates icon will bring the user to the following page. Here the user can see updates available, the date of the update check and the date of last update installation. The “Check Updates” buttons can be clicked to force an update check. The “Update System” will install the updates listed in the “Current available updates” window. **Note** that updates carried out here will **not** affect the API Gateway software version.

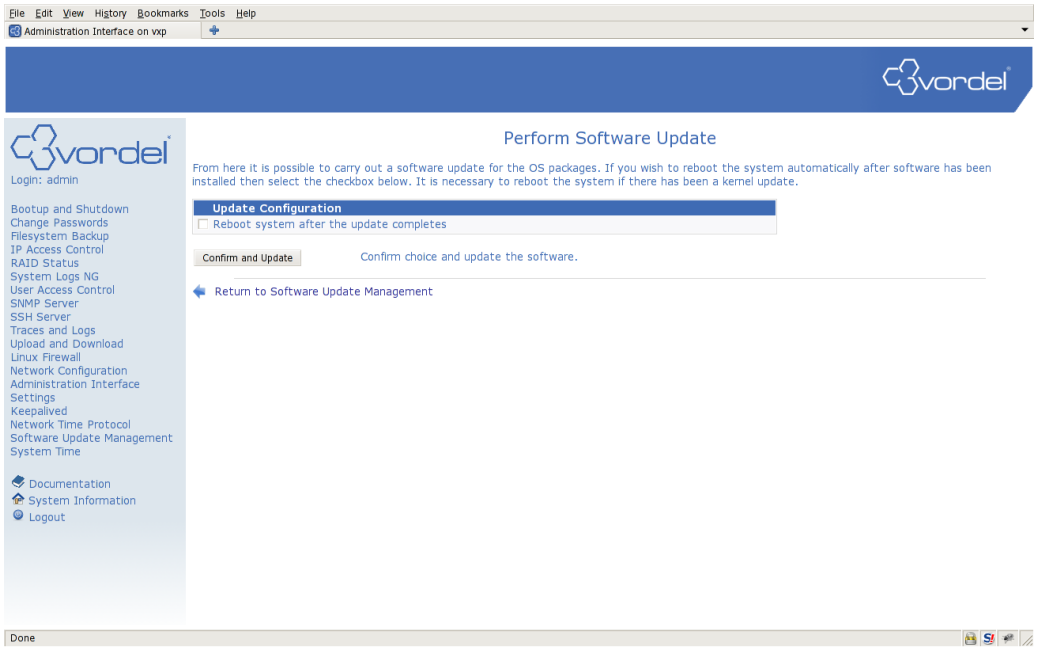


From this page it is also possible to change the schedule for automatic software update checks. By default these are run every Sunday night. To change the schedule click the green arrow next to “Edit Software Update Check Schedule”
Here the User can set a simple schedule (hourly, daily, weekly etc) or a more complex time similar to a

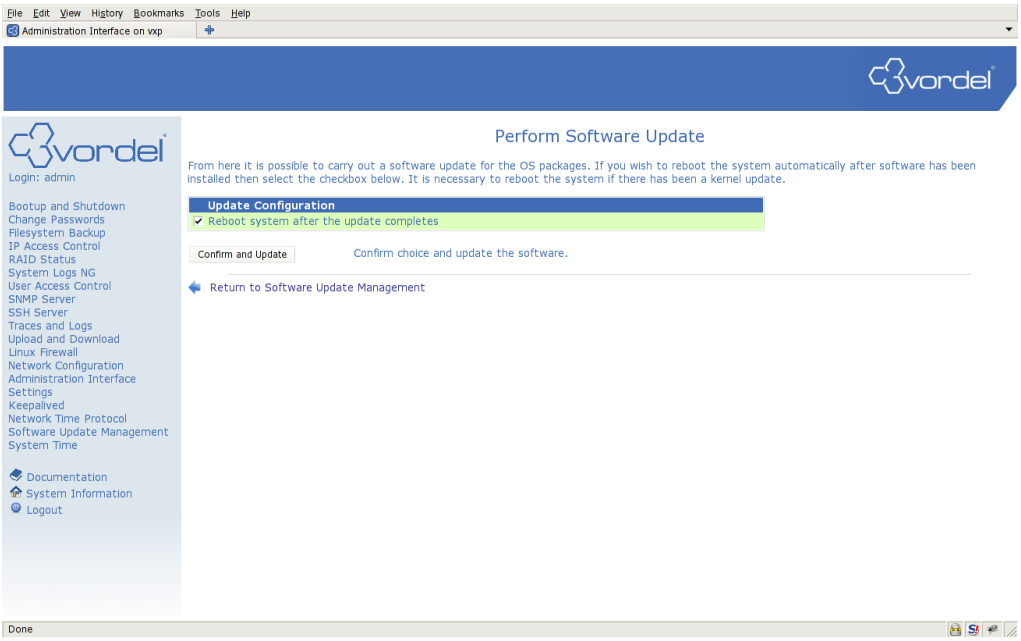
cron task. It is recommended that a suitable email address is entered in the “Email scheduled output” box. Click Save after making any modifications.



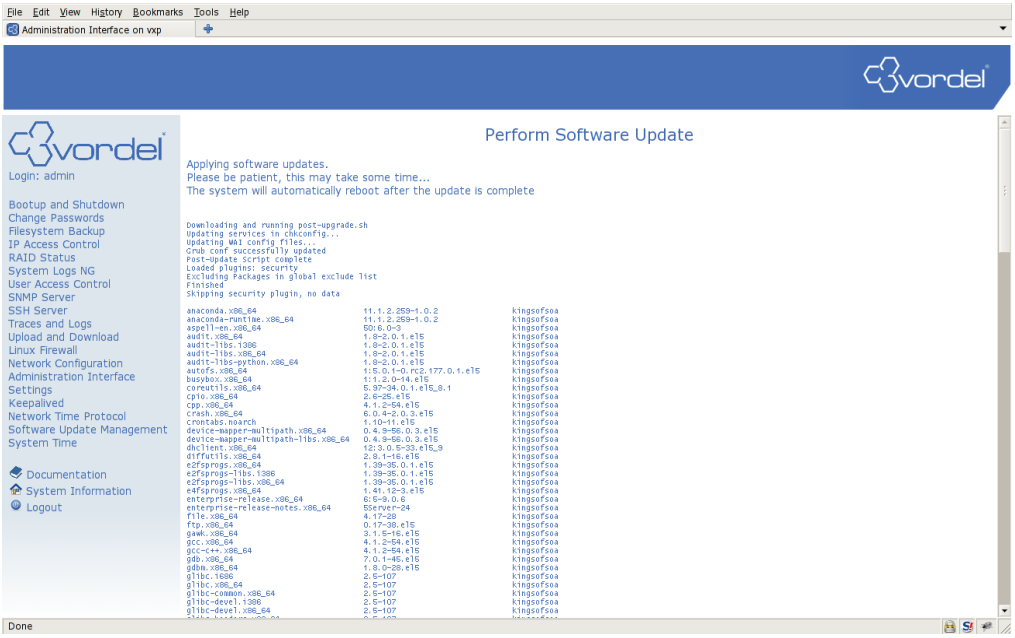
To Update any available updates click the “Update System” button.



If possible it is recommended to enable the Reboot system after update checkbox. Then click “Confirm and Update”



This will bring up the following page. Note the package update list will more than likely differ from below. Also, the package update list appears after the update, so may take some time to display.



Installing packages on Systems prior to v7.1

Note that the WAI module and system update scripts must be installed on a pre v 7.1 appliance. Run the following command when logged in as the root user. For more details please see the section on yum.

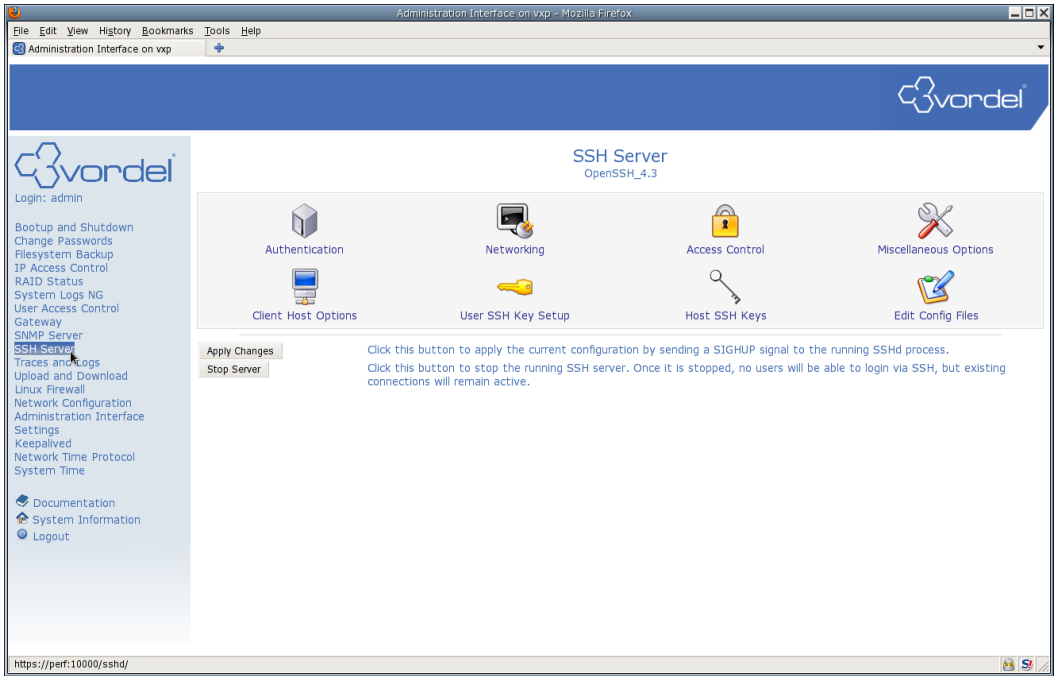
```
# yum install -y appliance-yum wbm-vordel-yum
```

Allowing root ssh access

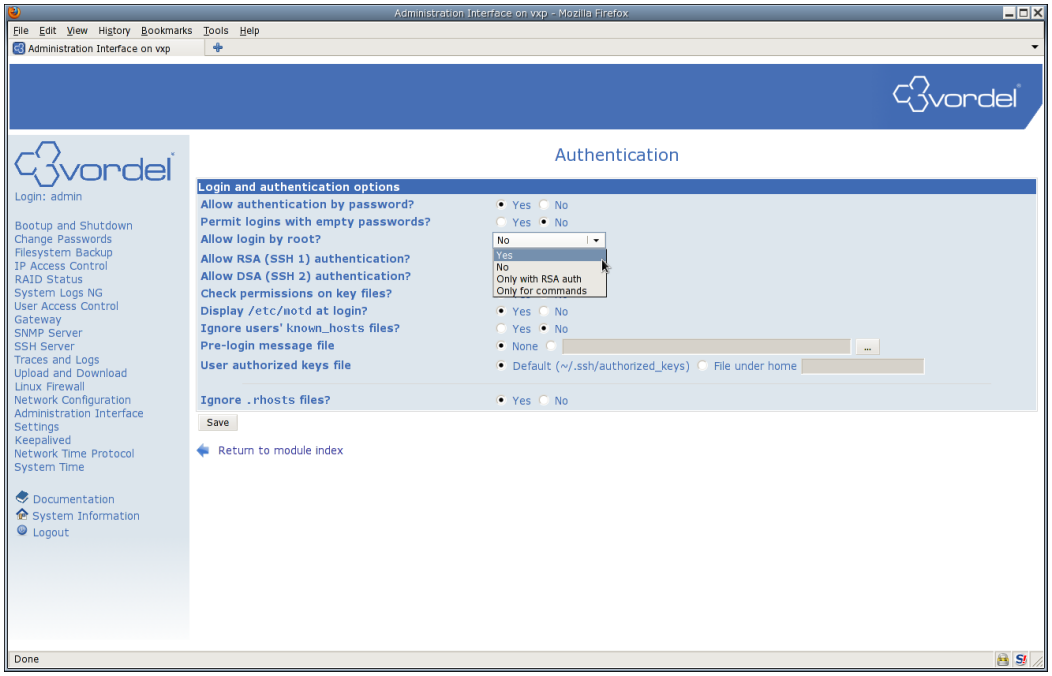
As a security feature direct ssh access by the root user to the Appliance is forbidden. For root access, the user must first log in as an unprivileged user (example `admin`) and then switch user to `root` using the 'su -' command.

To modify the system to allow direct root access (not recommended) the user can make the following changes through the WAI.

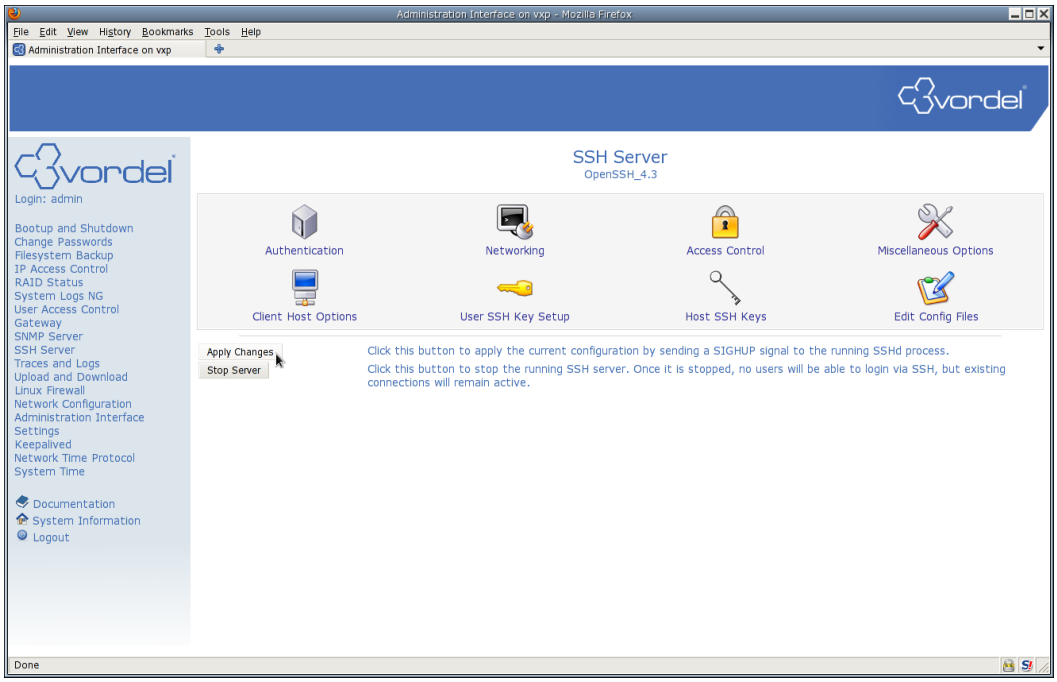
Log in to the WAI and select SSH Server from the menu on the left



Click the Authentication Icon and click the drop down box next to "Allow login by root?"
Select Yes and click the Save button



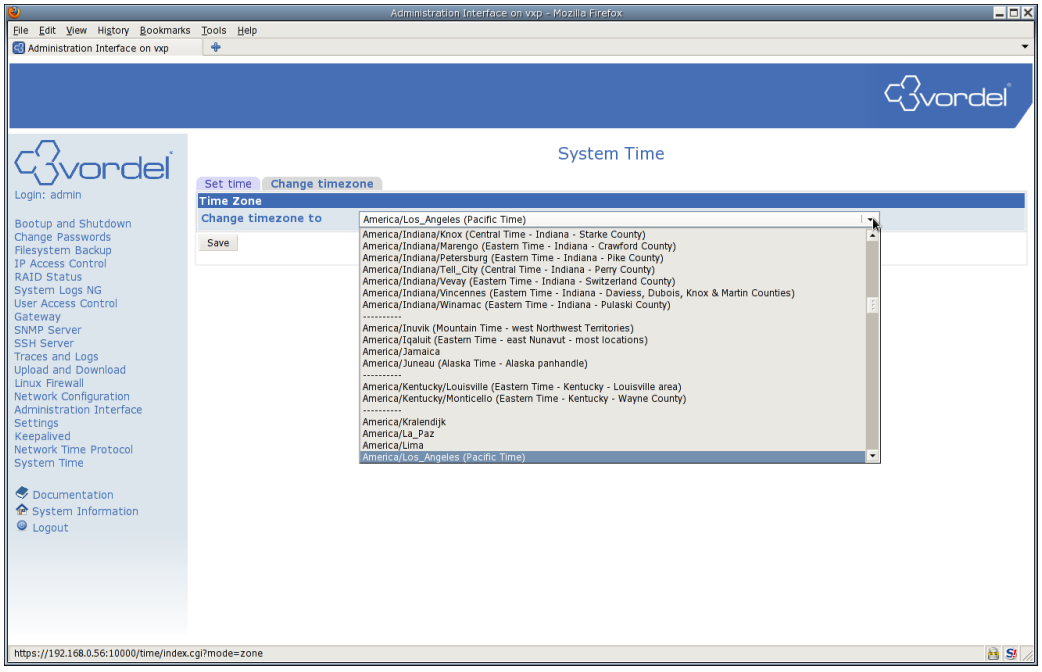
This will return you to the main SSH Server page. Click Apply changes for the changes to take effect.



Time and Date

Change Timezone

The default Timezone is PST. To change this follow these steps:
Log in to the WAI and select System Time from the menu on the left. Select the Change Timezone tab.

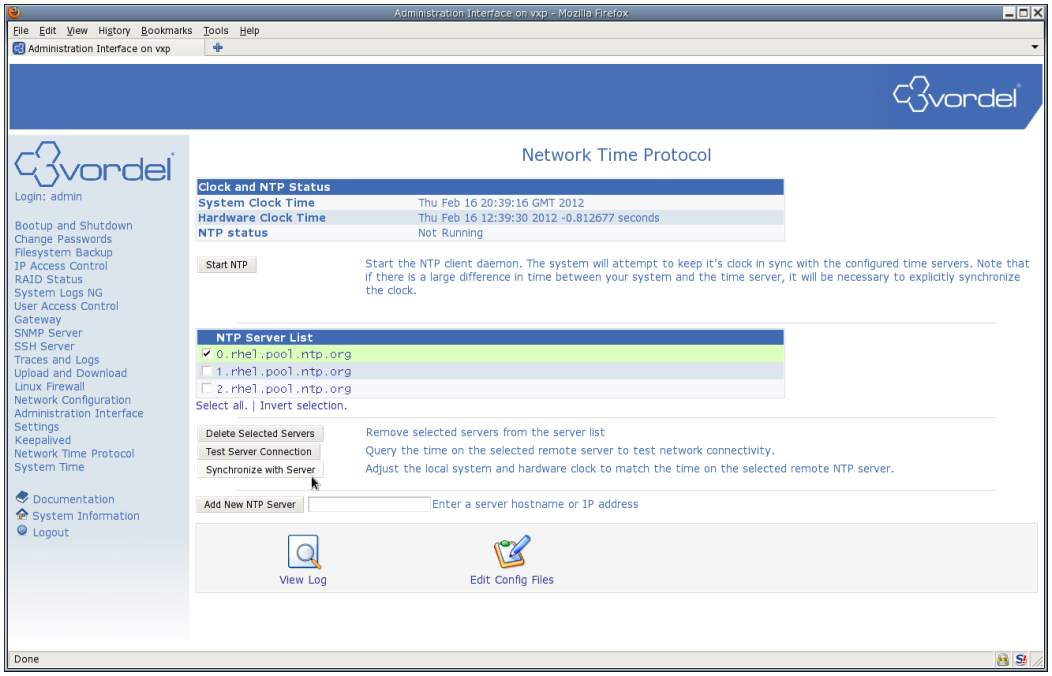


Here you can select your particular timezone from the dropdown list.
Click Save to set the new timezone.

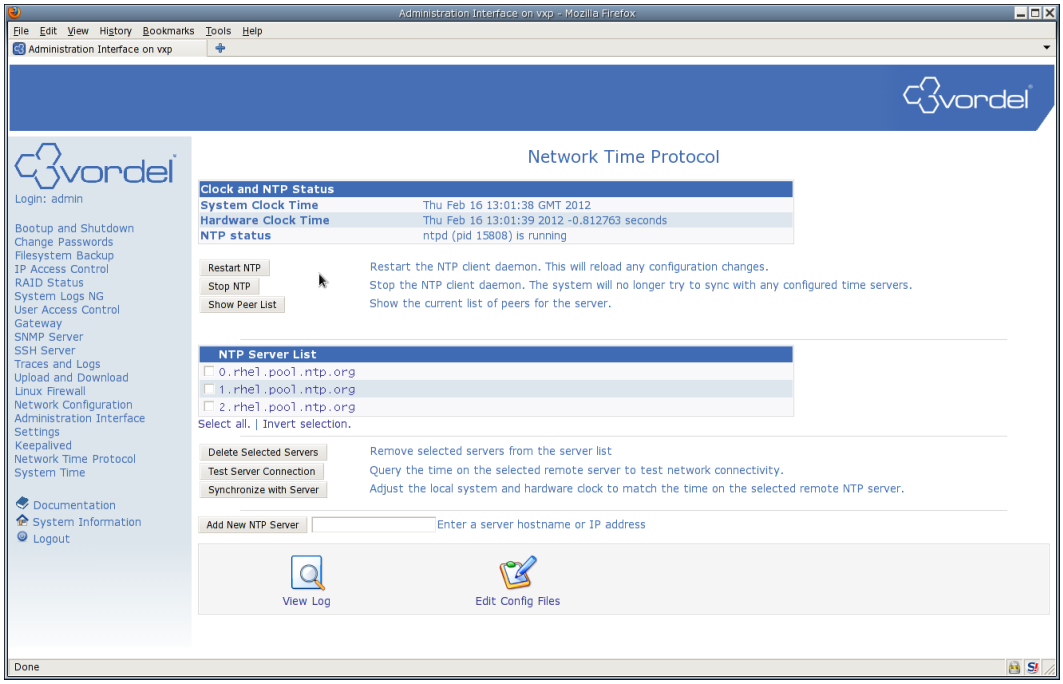
Configure NTP

NTP is available but not running by default on the Appliance. Clicking the Network Time Protocol menu link in the WAI will bring up a status page and allow the user to test connection to the currently configured NTP server, add their own server, and synchronize the clock to a given server. It is recommended that the user synchronize the system clock with a server before starting the NTP daemon.

Log in to the WAI and select Network Time Protocol. Select a server on the list and click Synchronize with Server.

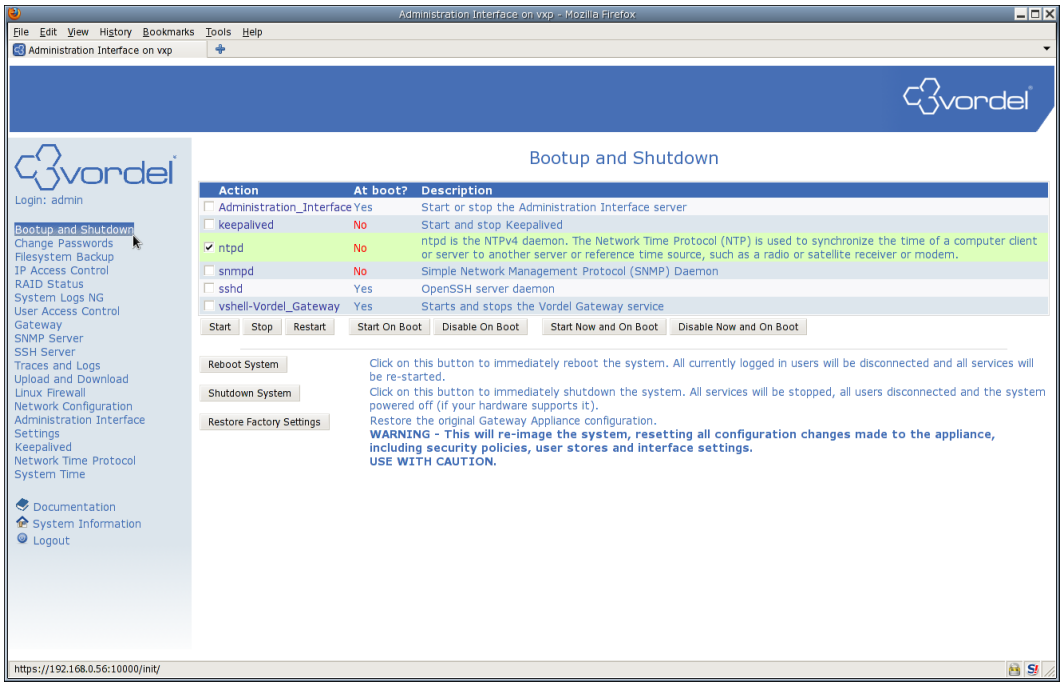


After the server synchronizes the time successfully, click the Start NTP button. The status page will update with details of the NTP daemon process id, and give further options to query the state of NTP.

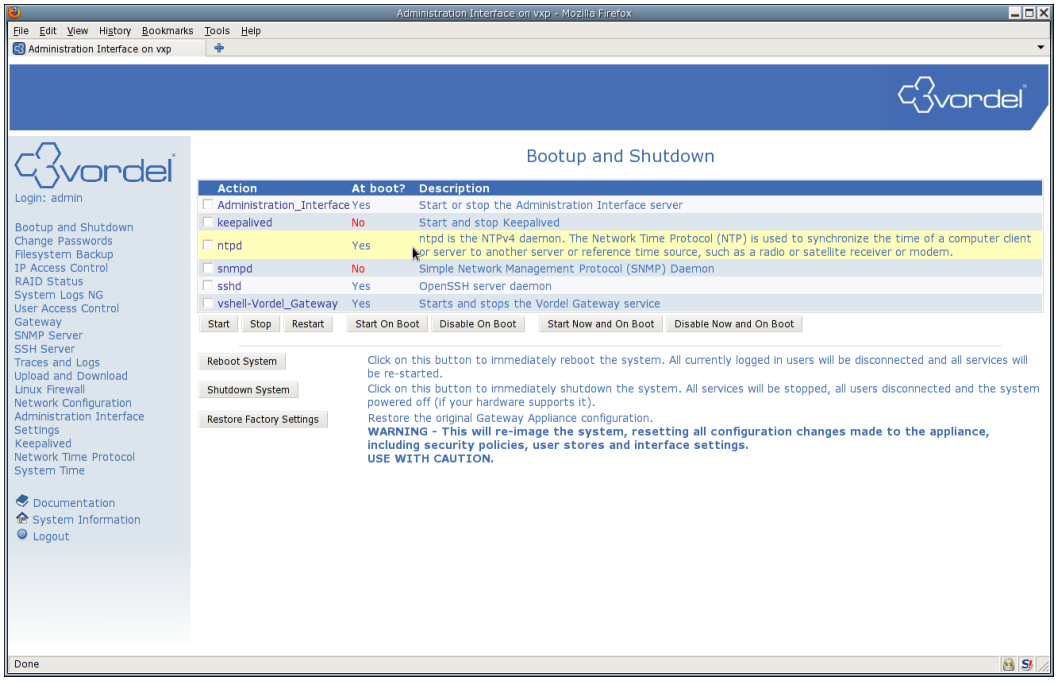


To automatically have the NTP daemon start after a system reboot you must adjust the service in the Bootup and Shutdown menu.

Click on the Bootup and Shutdown Menu item and select the checkbox next to ntpd. Then Click the Start On Boot button.



The page should update as follows with Yes in the “At boot?” column for ntpd



Firewall

The Appliance is configured with an active Firewall by default. This restricts unauthorized access to the

system on a majority of TCP and UDP ports.

Default Ports

In version 6.3.1 the default open ports on the Appliance are as follows

SSH	TCP 22
Gateway	TCP 8080, 8090
HTTP	TCP 80
HTTPS	TCP 443
Web Administration Interface	TCP 10000
NTP	UDP 123
SNMP	UDP 161
LDAP	TCP 389
LDAPS	TCP 636
Oracle DB	TCP 1521
MySQL DB	TCP 3306
Cassandra Cluster Port	TCP 7000

VRRP to 224.0.0.18 is also allowed to ease configuration of keepalived.

Earlier versions will not have HTTP/S, LDAP/S and the DB ports open by default.

Differences between Appliance releases

Note that between version 6.2.0 and 6.3.0 of the Appliance the “Chain RH-Firewall-1-INPUT” has been removed and all the rules have just been set as input rules. It is only a slight cosmetic change but is something to bear in mind when following the instructions below. The latest Appliance documentation should always be referenced for the most up to date changes.

Also, for versions of the Appliance prior to 6.3.0 the Firewall WAI menu is not enabled by default. To enable it the user must run the following command as root:

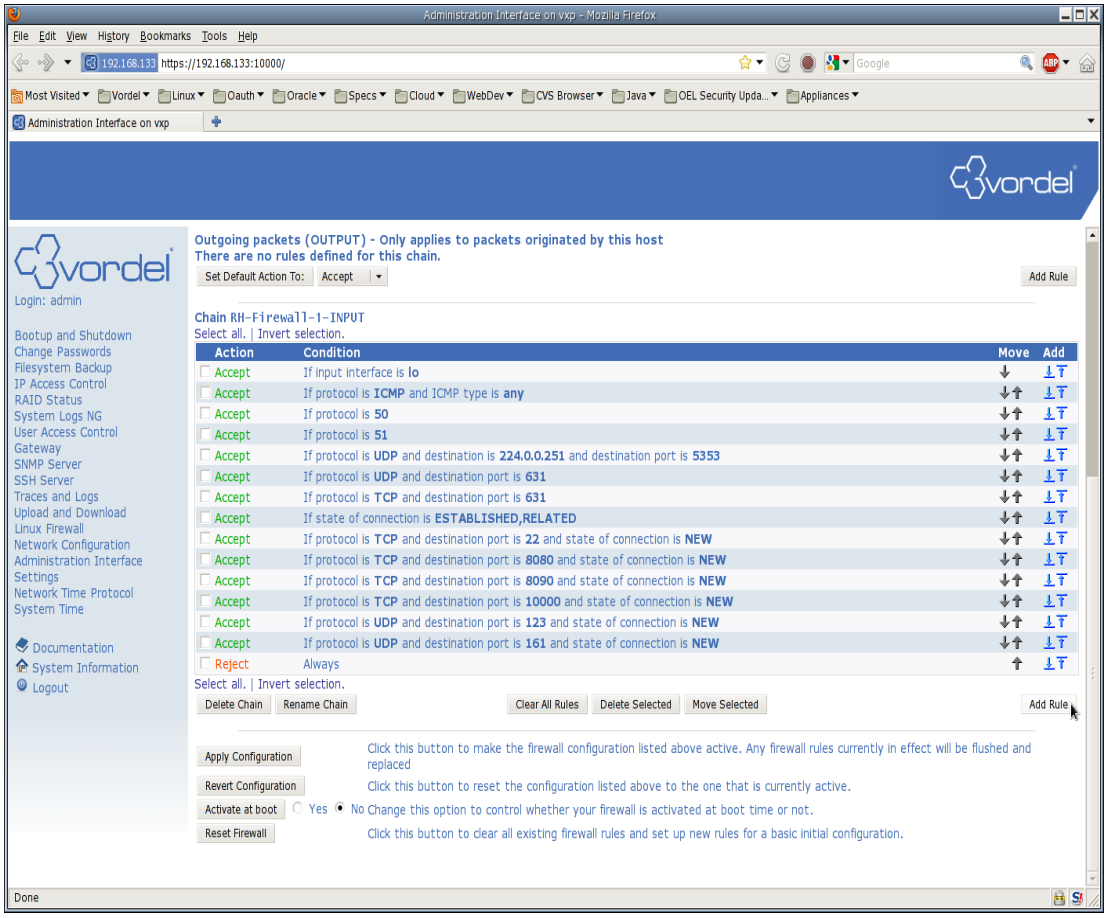
```
# sed -i '/firewall/!s/vordel-access-control/vordel-access-control firewall/' /etc/webmin/webmin.{acl,groups}
```

Opening new ports

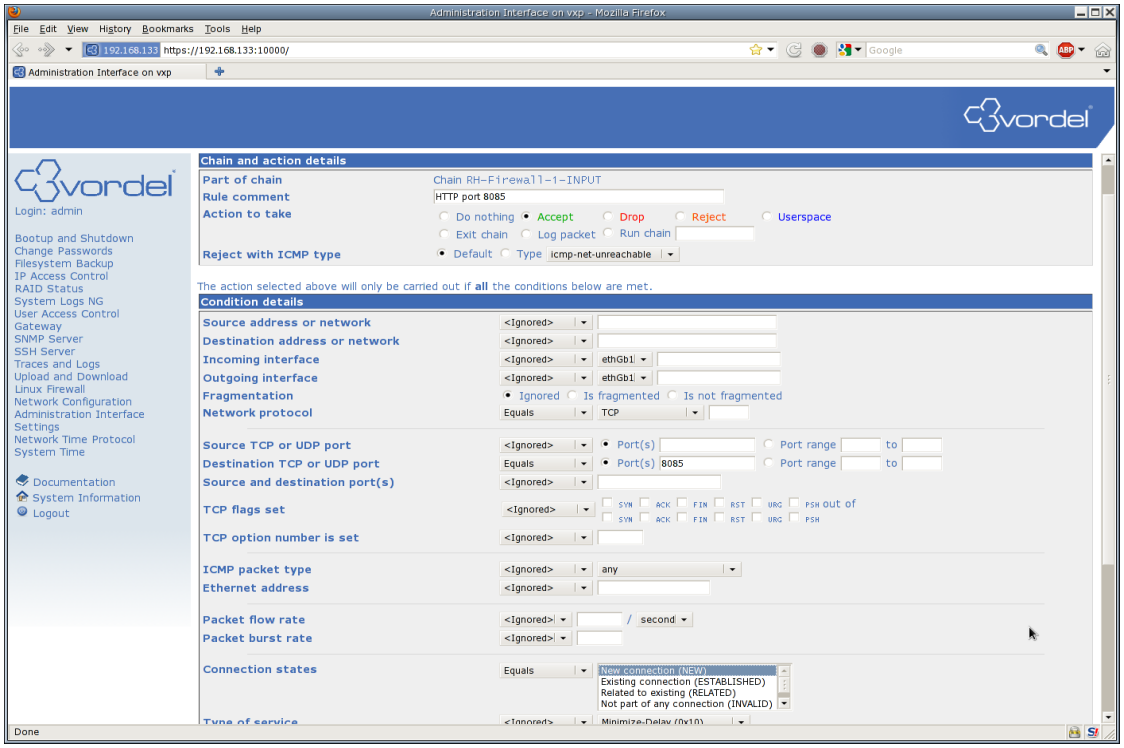
For this example a new HTTP port 8085 is going to be opened to accept incoming traffic on the appliance. If you wish to open a different port then replace 8085 in the steps below.

1. Select the "Linux Firewall" module
2. Scroll down the page to the "Chain RH-Firewall-1-INPUT" section. It can be easily identified by the table of existing Accept and Reject rules.

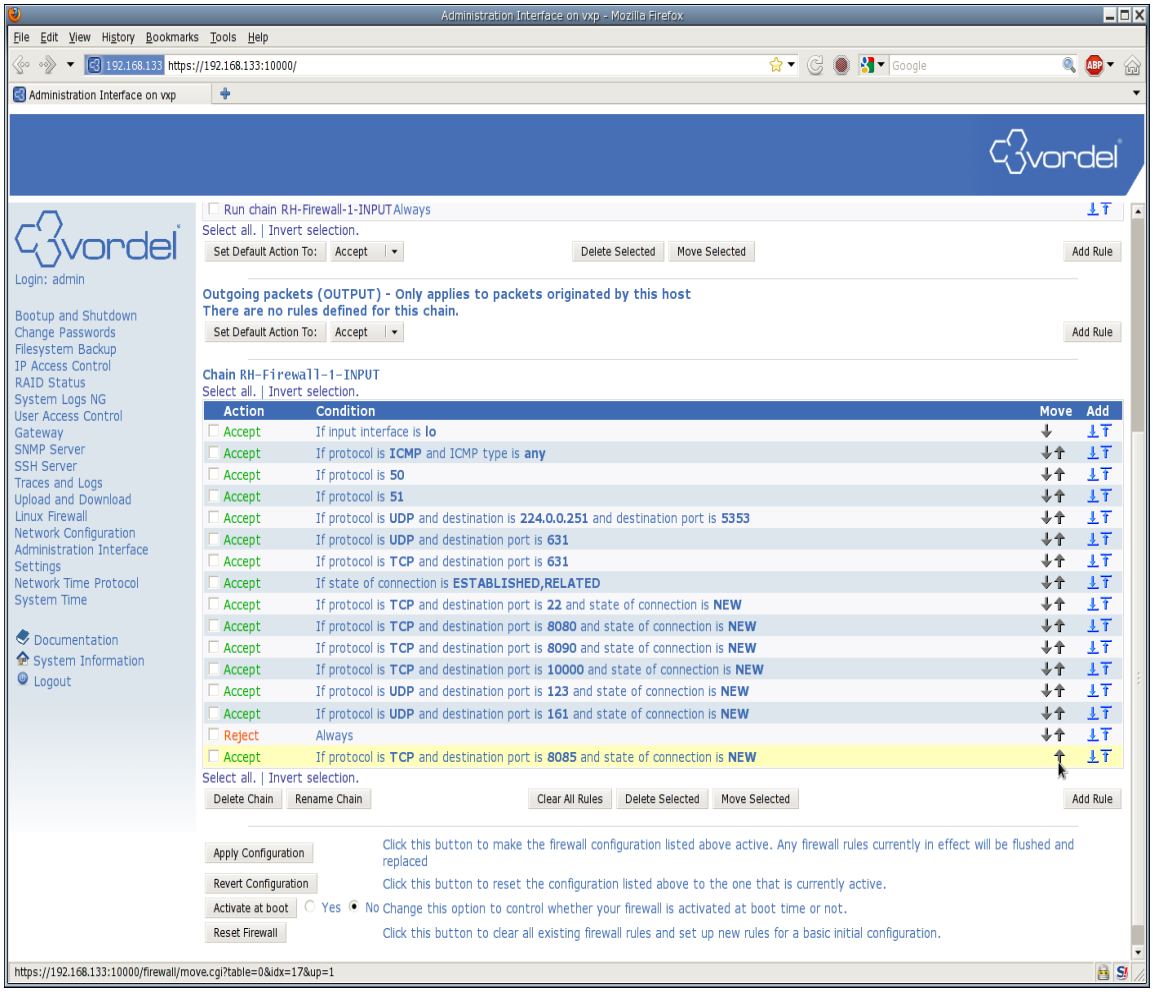
3. Click the "Add Rule" button near the bottom right hand corner of this rule table. This will bring up the Add Rule page.



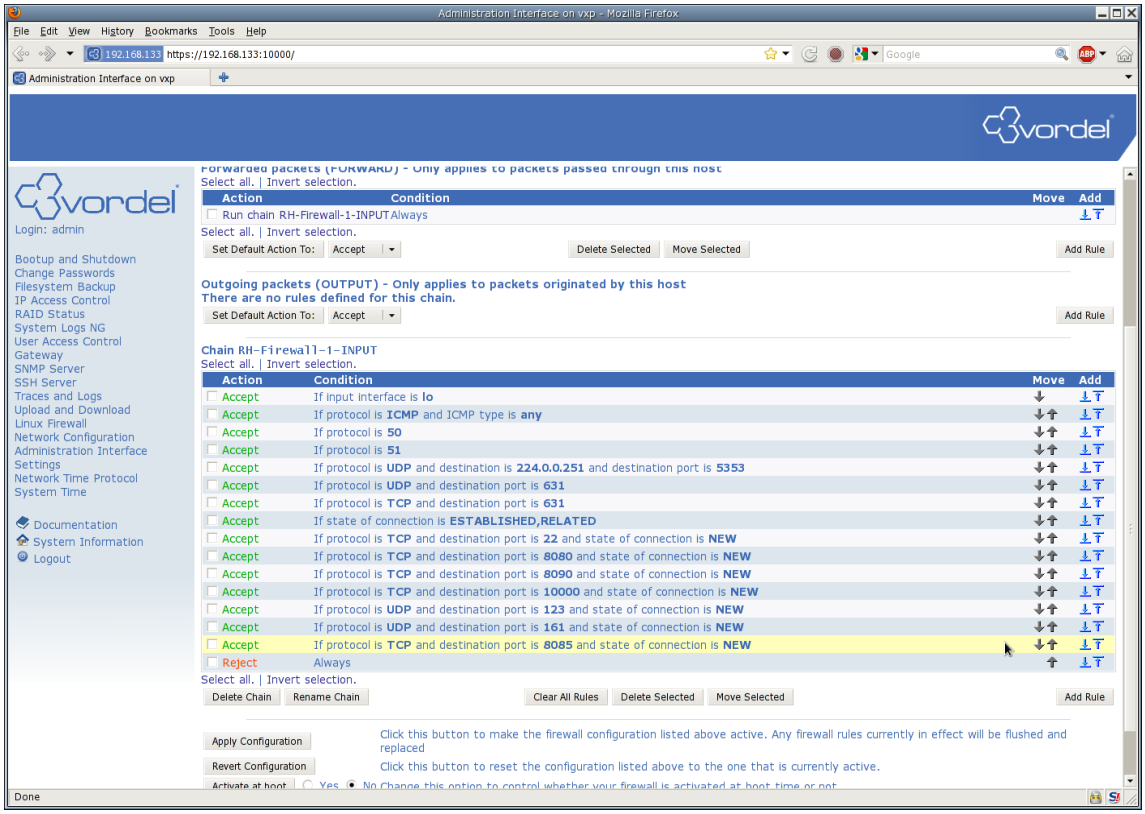
4. In the "Chain and action details" table you can enter a comment to identify the use for the rule. This could be "HTTP port 8085"
5. In the "Action to take" section click the "Accept" radio button.
6. Scroll down to the "Condition details" table. Here it is possible to restrict traffic based on a number of conditions. For this example it is only required to open the port 8085 without restrictions. Therefore a lot of the choices can be left at the default.
7. Change the "Network protocol" dropdown fields to "Equals" and "TCP"
8. Change "Destination TCP or UDP port" dropdown field to "Equals" and select the "Port(s)" radio button. In the "Port(s)" text input field enter "8085"
9. Change the "Connection states" dropdown field to "Equals" and select "New connection(NEW)" in the select box.



10. Scroll down and click the "Save" button on the bottom left of the page. This should bring you back to the "Linux Firewall" page and your new rule should now be seen at the bottom of the "Chain RH-Firewall-1-INPUT" table.



11. Click the upward arrow in the "Move" column next to the new rule so that the new rule is above the "Reject Always" rule.



12. Click the "Apply Configuration" button near the bottom of the page to allow the configuration changes to take effect.

Please see this document for further usecases.

Configuring the Firewall using CLI

It is also possible to configure the firewall using the CLI while logged into the appliance as the root user.

For users familiar with iptables this may be a quicker and more powerful way of creating and managing their firewall. iptables is a very powerful and somewhat complex program, documentation of all its commands is beyond the scope of this document. For a command reference please see this following link:
http://linux.die.net/man/8/iptables

Note for users without strong iptables knowledge, the recommended method of configuring the firewall for the appliance is through the WAI.

Modifying Network Configuration

This describes the configuration steps necessary to modify the default network card configuration on an Appliance to a more typical customer requirement. The steps are outlined using the Web Administration Interface to make system modifications. The purpose of the reconfiguration is to have each of three network interfaces residing on a different network.

These networks correspond to:

- An Administration network (behind the inward facing firewall)
- The inbound network (external traffic inbound to the Gateway)
- The outbound network (traffic destined for the Intranet, outbound to the Gateway)

For the purposes of the example the following IP addresses will be used

Network	CIDR IP Address
Administration	**192.168.0.10/24**
Inbound	**200.0.0.10/24**
Outbound	**10.0.0.10/24**

These IP addresses are given as an example only and should be changed to suit the particular network topology.

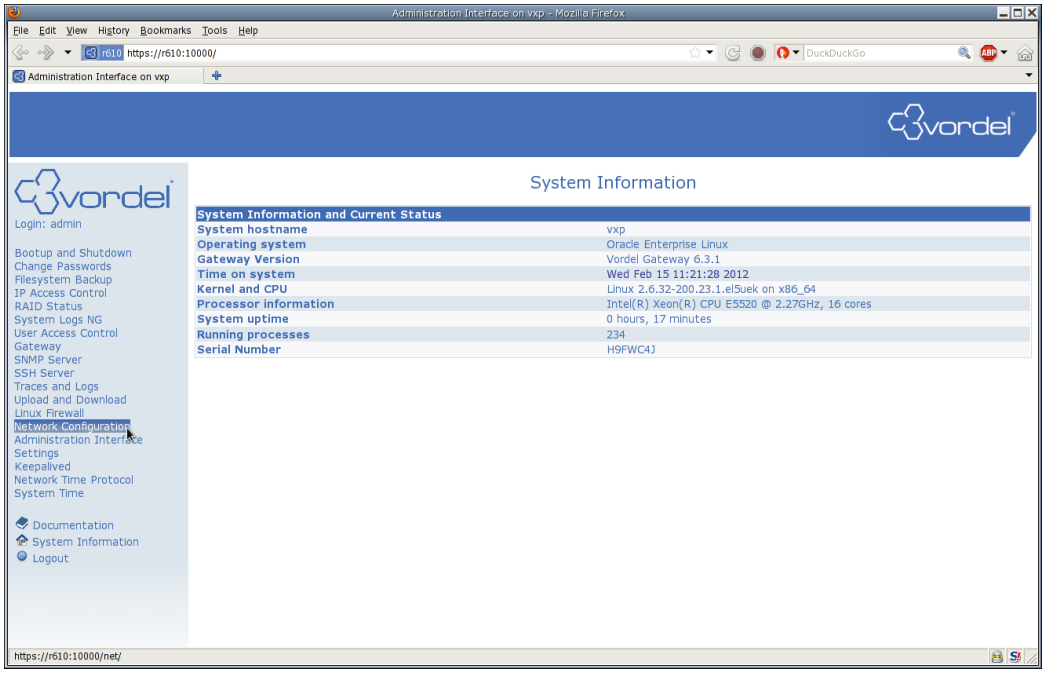
It is recommended that the ethGb1 interface is used as the Administration interface if possible. This is due to the fact that management of the Dell iDRAC controller is shared on this physical interface.

Default Network Settings

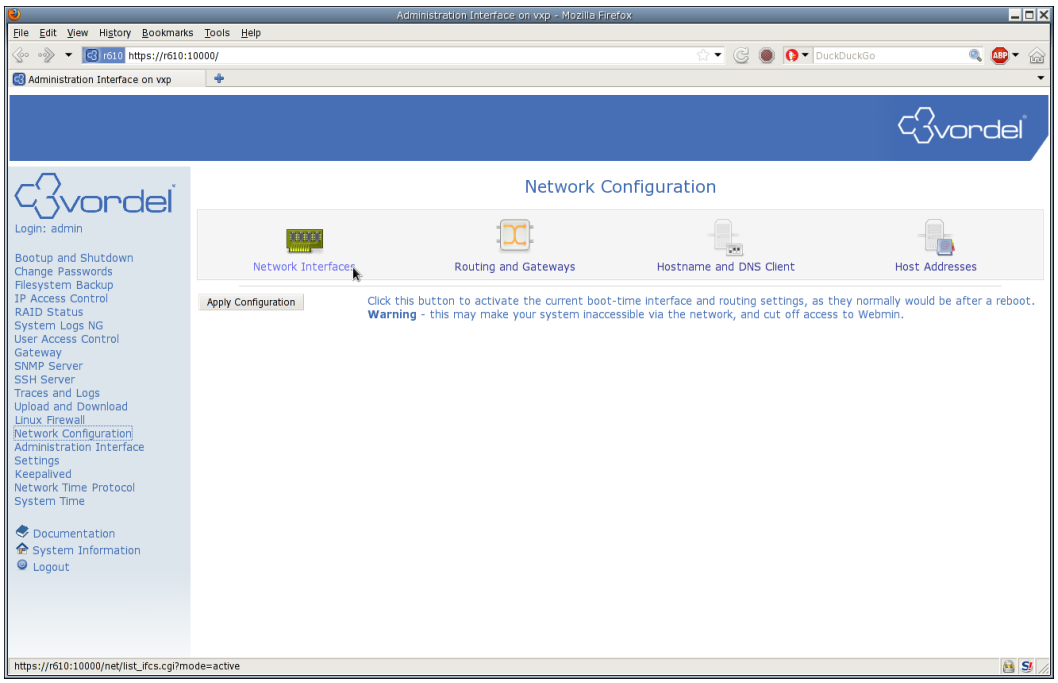
By default the Appliance ships with two network interfaces enabled: ethGb1 and ethGb2.
The device ethGb1 is configured to use DHCP, and ethGb2 is set up with the static IP address 192.168.200.200.

Modifying Network Configuration

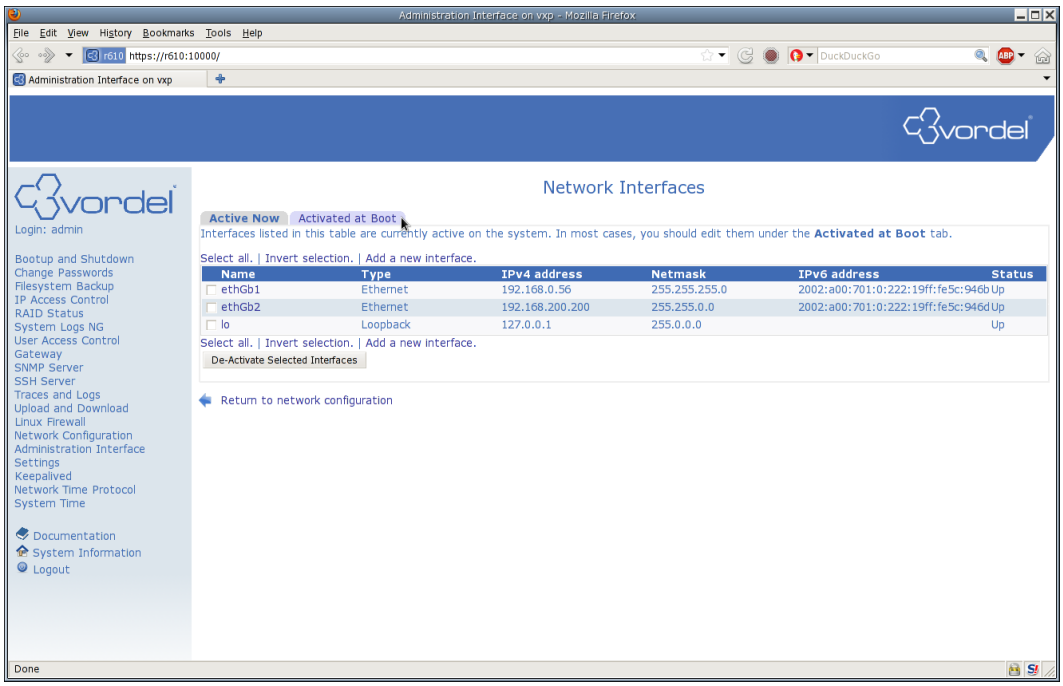
Log in to the WAI and click on “Network Configuration” in the menu on the left



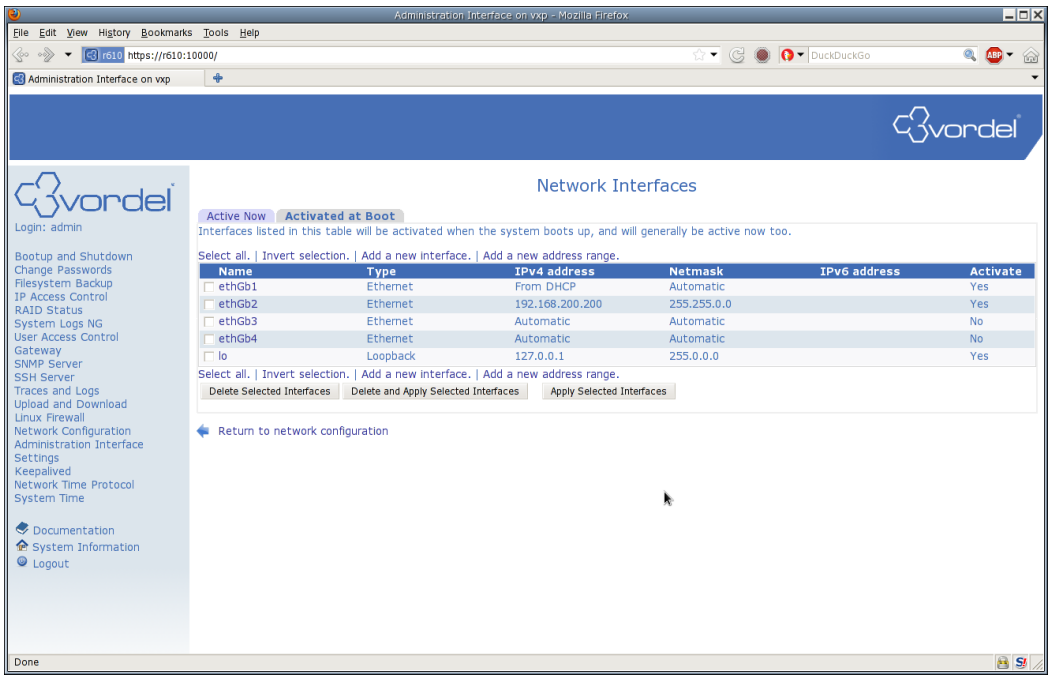
In the Network Configuration screen click on the Network Interfaces icon.



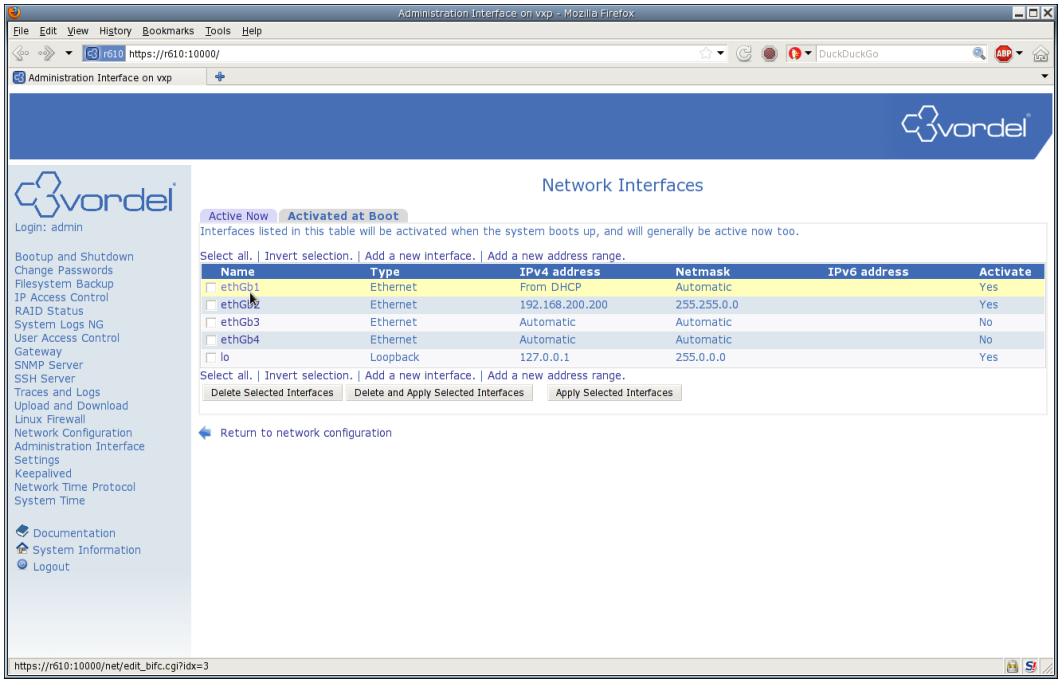
In the Network Interfaces screen click on the Activated at Boot tab



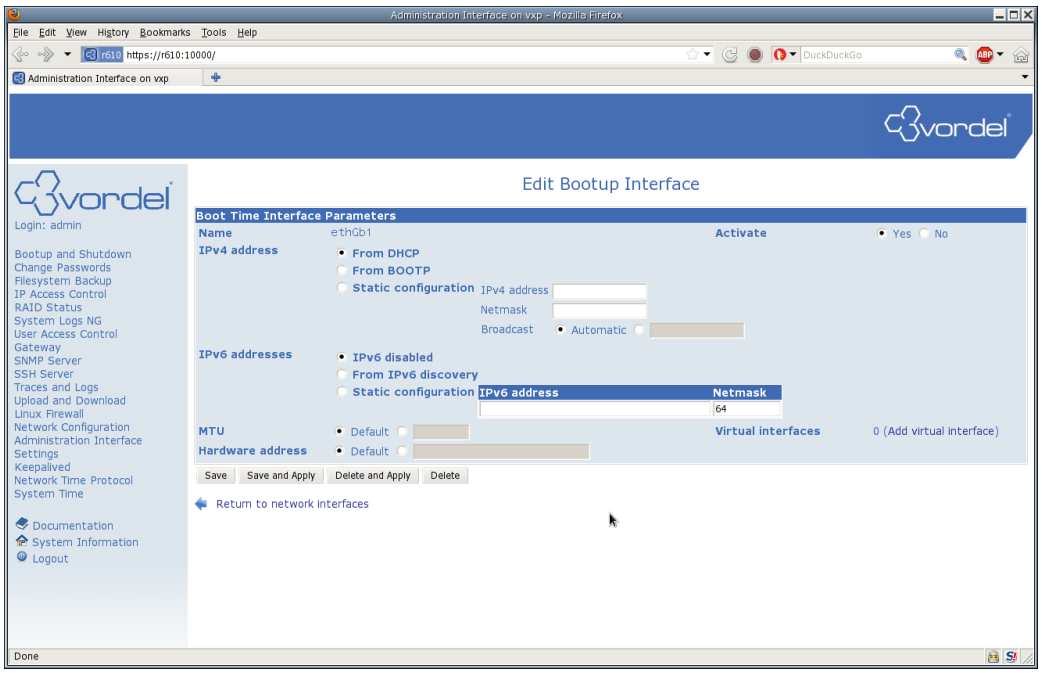
Here you can see the default configuration for the Interfaces on the Appliance.
The device ethGb1 is configured to use DHCP, and ethGb2 is set up with the static IP address 192.168.200.200.



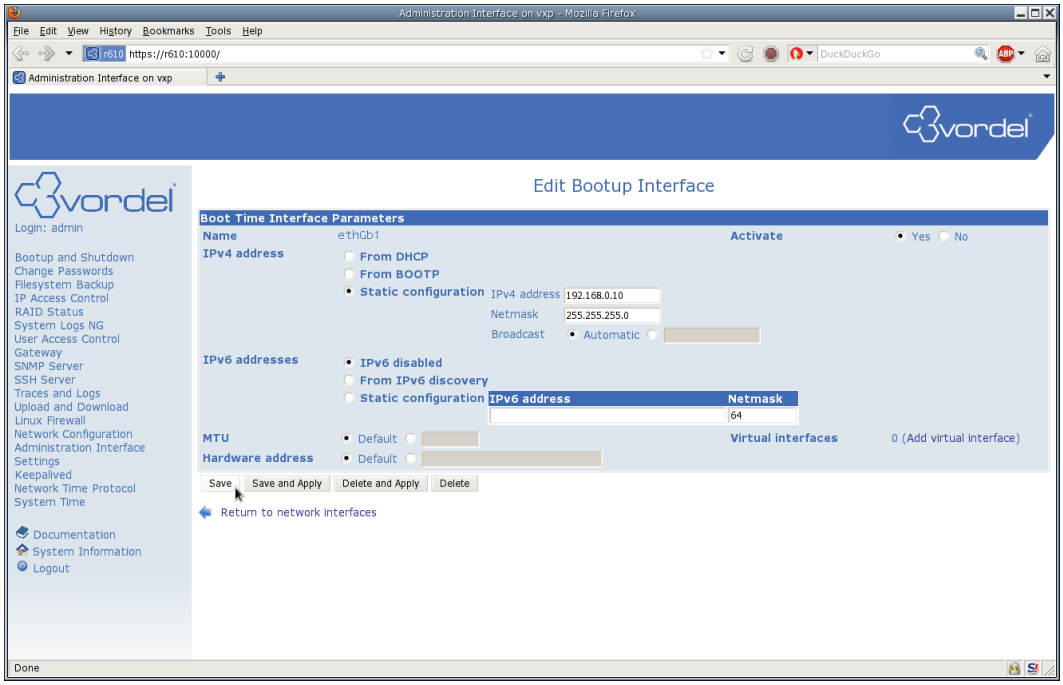
Select ethGb1 to configure it as the interface residing on the Administration network.



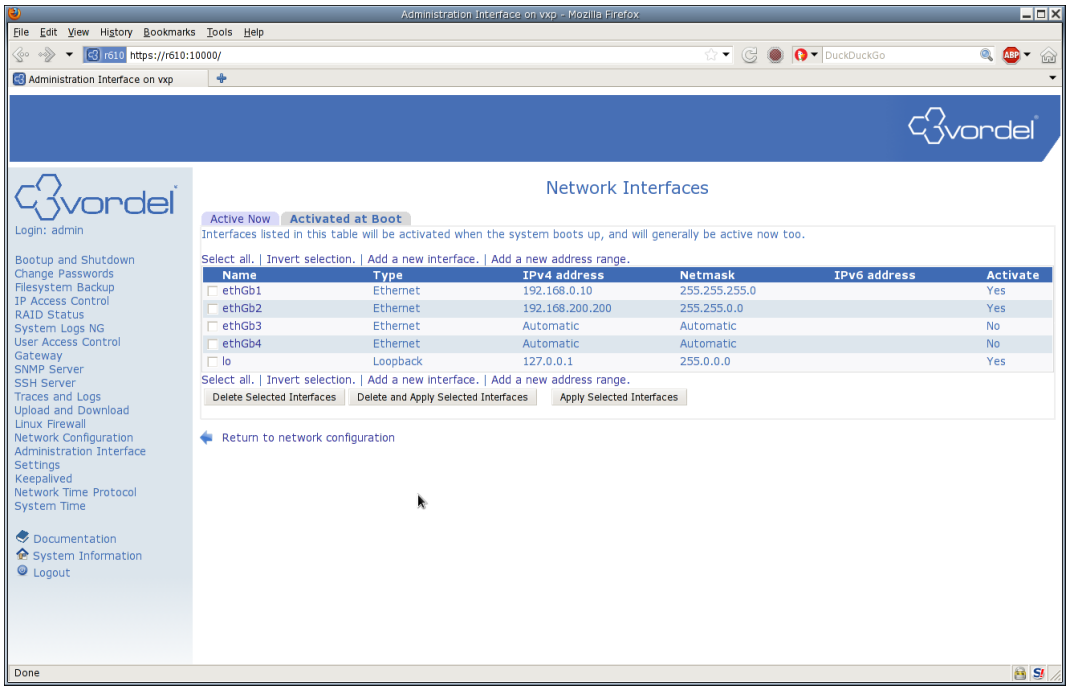
This will bring up the configuration page for that interface. By default it uses DHCP.



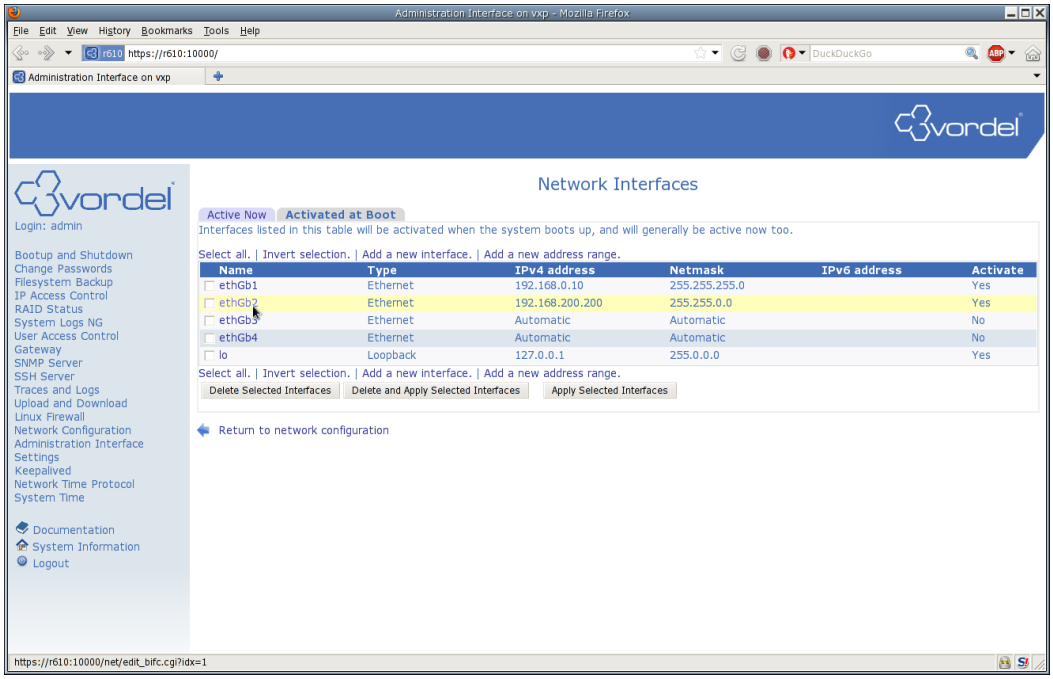
Select Static configuration and enter the new IP address and netmask. Select Automatic for the Broadcast address. Then click Save.



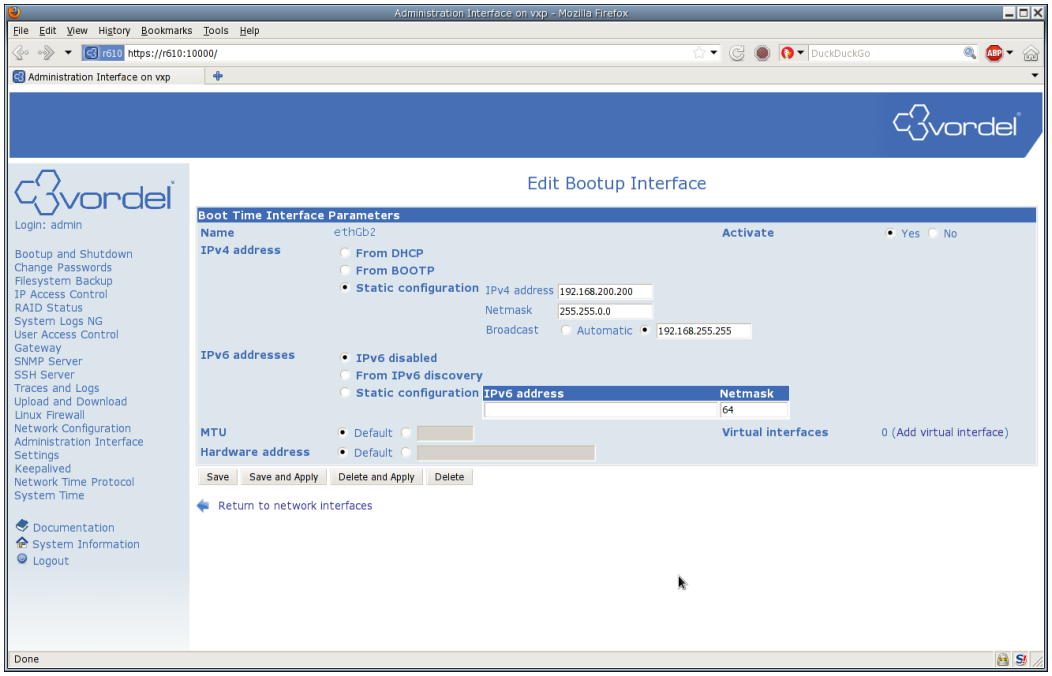
This will bring you back to the Network Interfaces screen. You can see the new IP address and Netmask for ethGb1



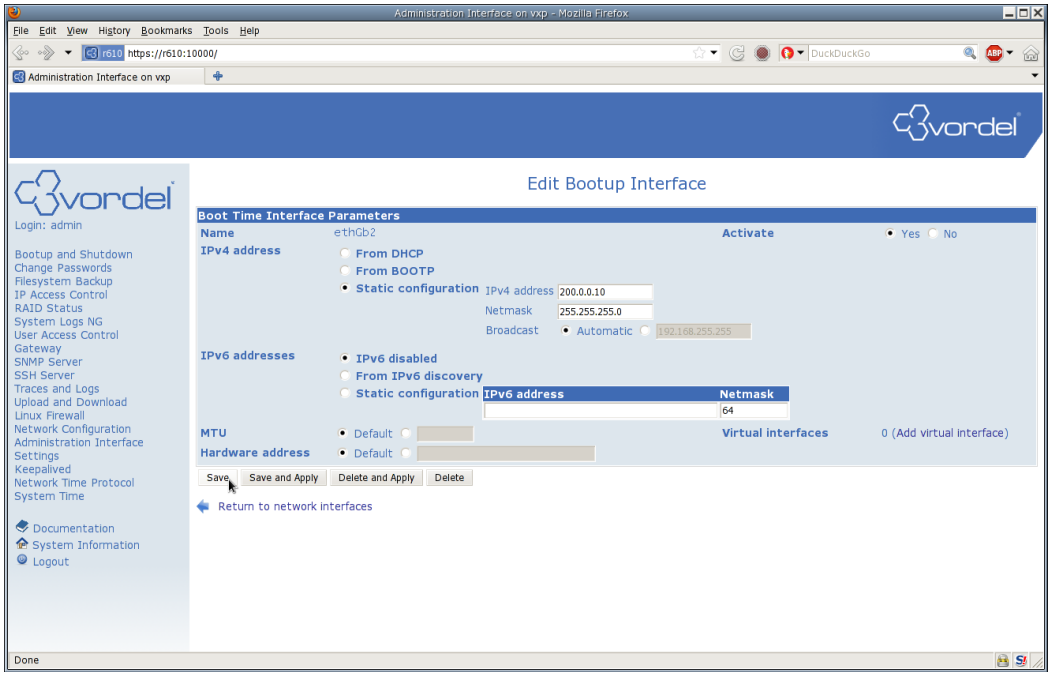
Repeat the procedure for ethGb2. Select ethGb2 to configure it as the interface residing on the inbound network.



By default it has the static IP address of 192.168.200.200.

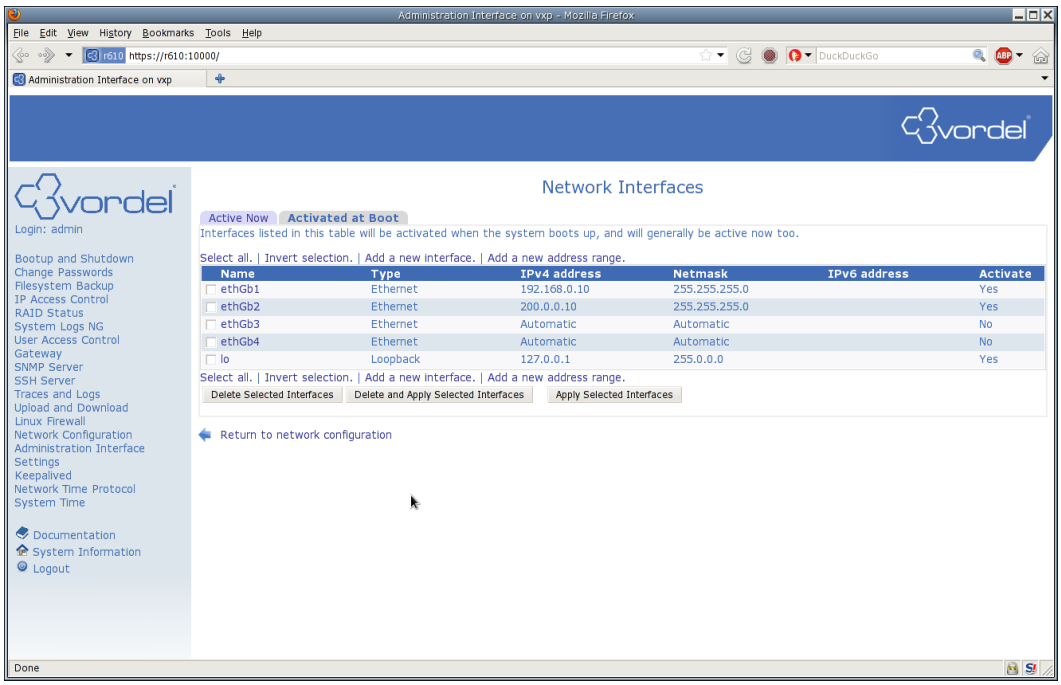


Change this to your inbound static IP address and click Save.

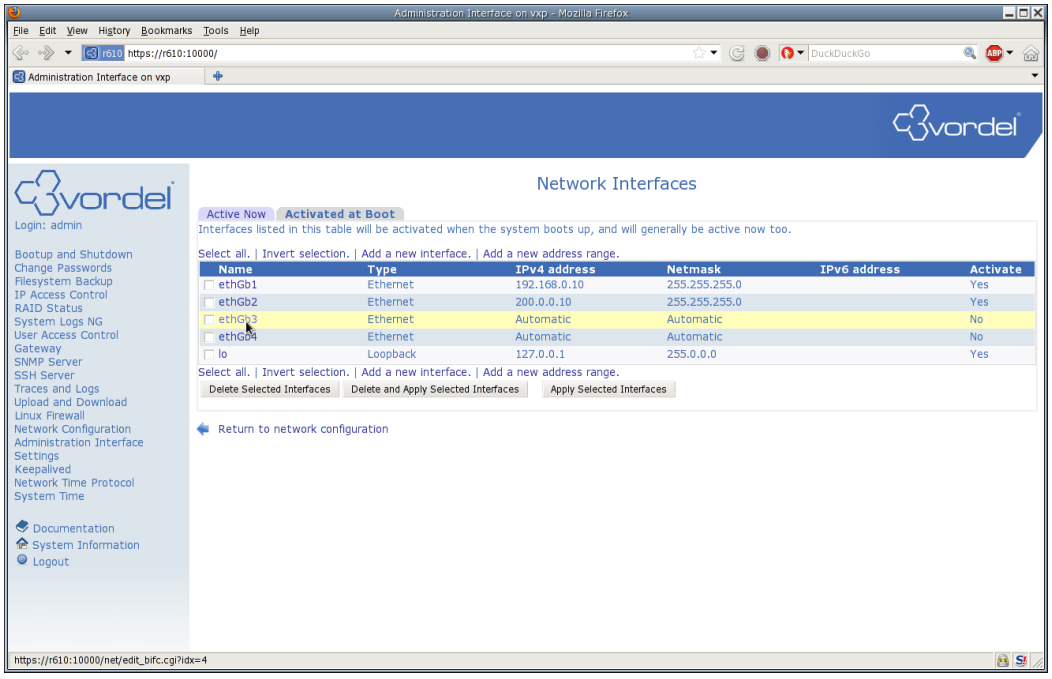


This will bring you back to the Network Interfaces screen. You can see the new IP address and Netmask

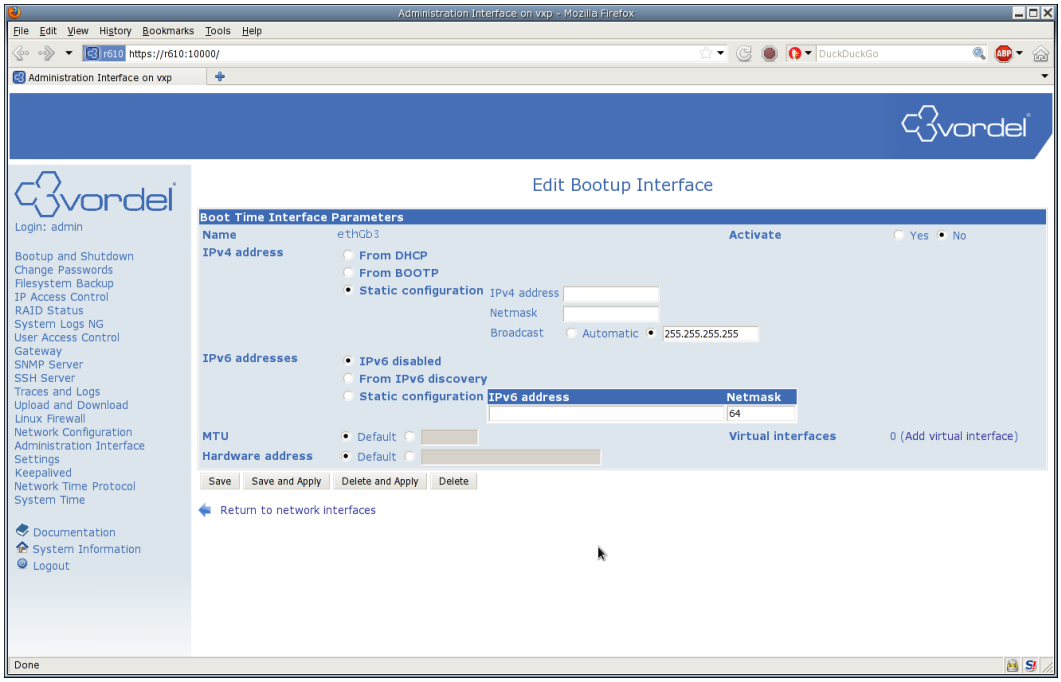
for ethGb2



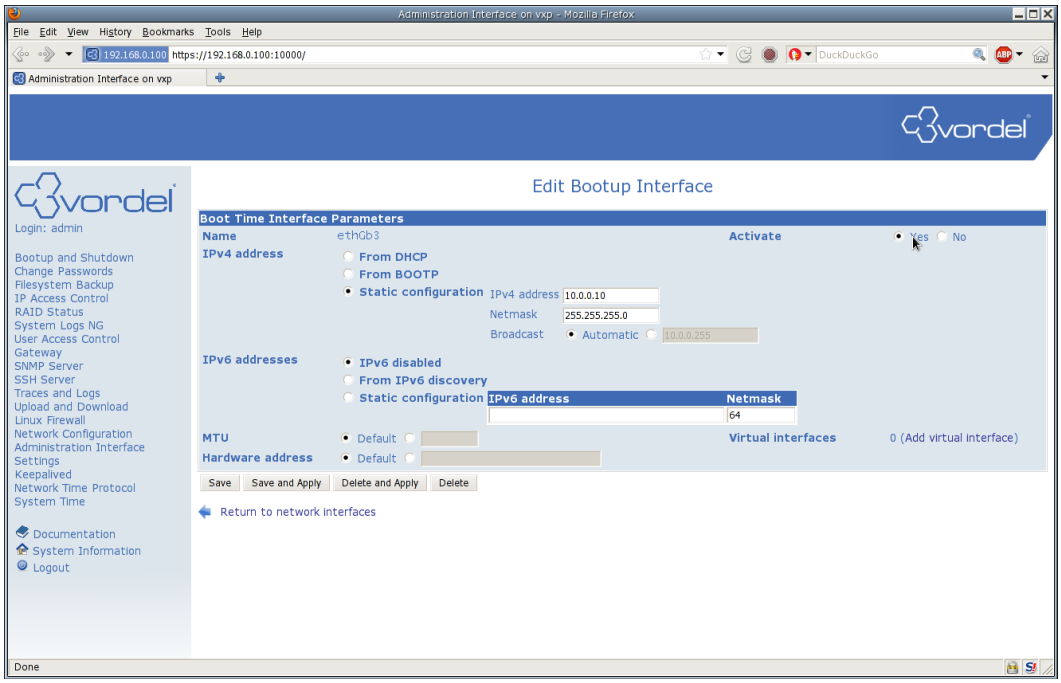
Repeat the procedure for ethGb3. Select ethGb3 to configure it as the interface residing on the inbound network.



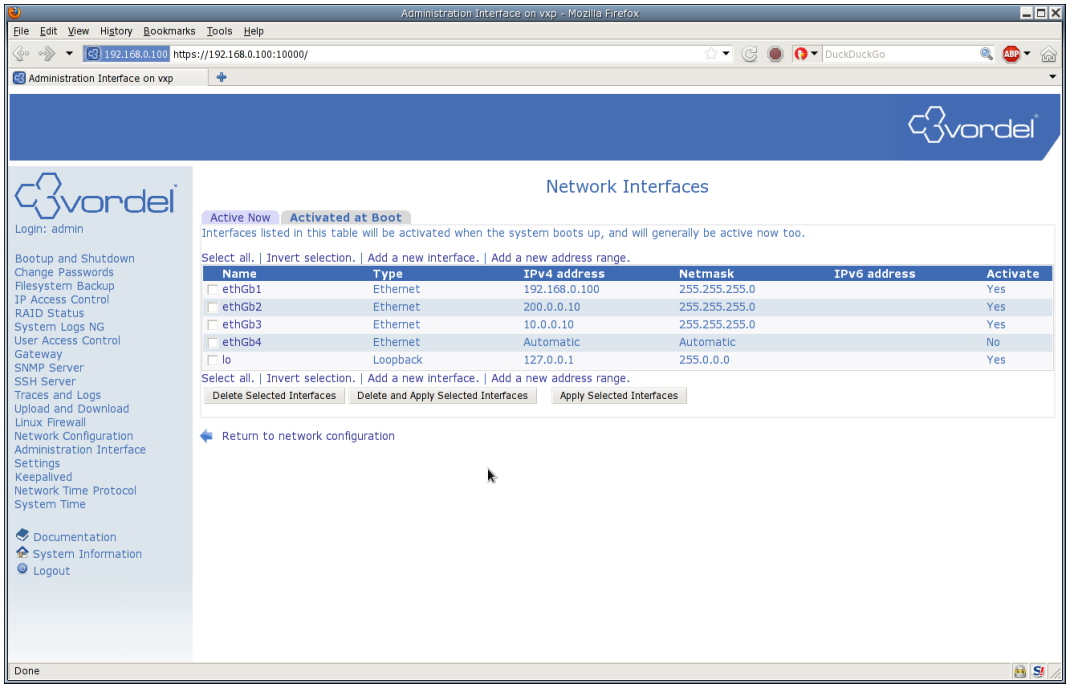
By default it does not have an IP address configured.



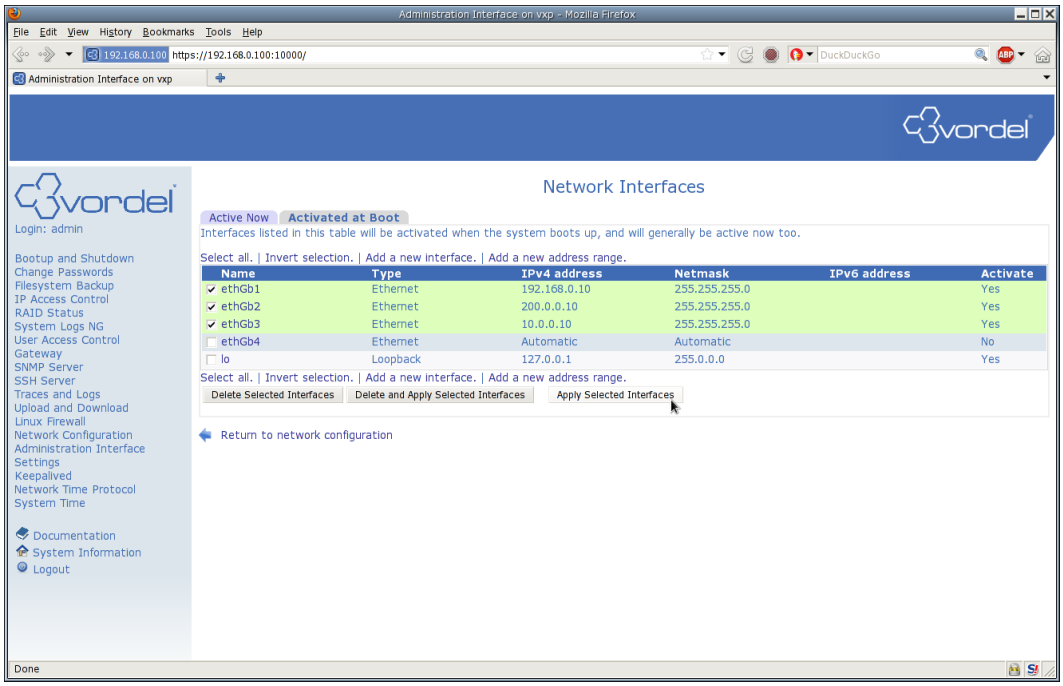
Modify this to enter you outbound static IP address. Note that by default this interface is not activated. You also have to change the checkbox in the upper right hand side to Activate Yes. Then click Save.



This will bring you back to the Network Interfaces screen. You can see the new IP address and Netmask for ethGb3. Note that the Activate column for ethGb3 is now set to Yes.

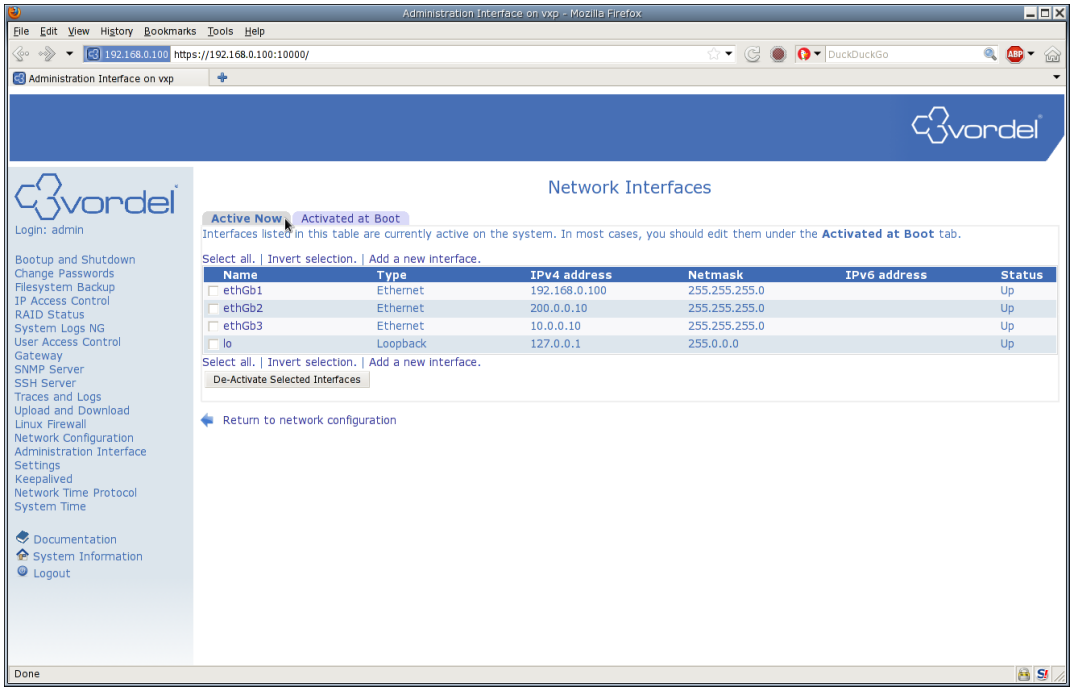


To apply the changes select the checkboxes next to the interfaces which you have changed and click the Apply Selected Interfaces button



Note that if your administration IP address has changed you may have to re-login to the Web Administration Interface.

Clicking on the Active Now tab in the Network interfaces screen will show the new IP addresses.



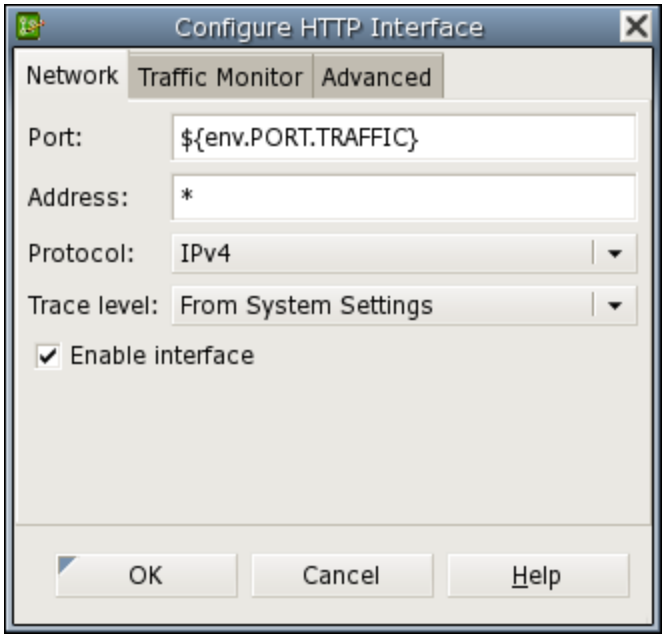
Interface Configuration on Gateway

After choosing which IP address the Gateway will listen for requests on (the inbound interface) you can configure the Gateway to only bind to this particular address. This way it is ensured that the Gateway will only listen for requests arriving on that network interface. By default, the Gateway will listen on all interfaces and addresses. Instructions here are given to restrict the pre-configured interface on Default Services.

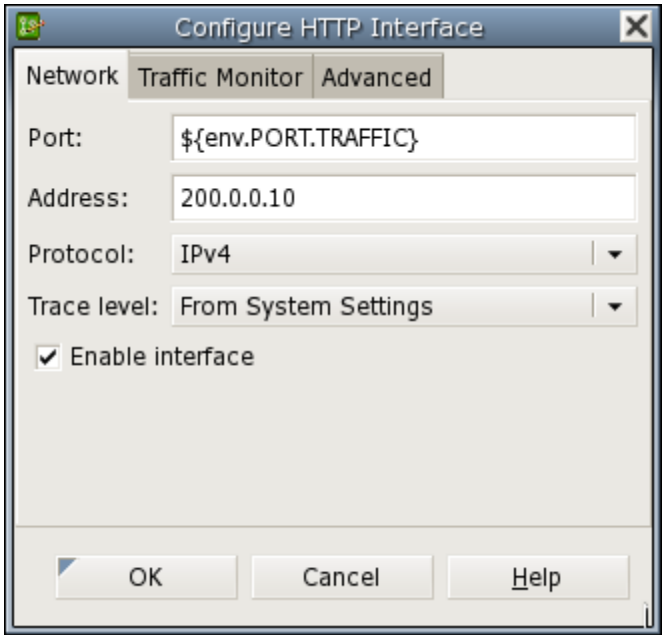
To make these changes you must connect to the Gateway using Policy Studio.

Perform the following steps:

- In the Policy Studio navigation tree, select **Listeners -> API Gateway -> Default Services -> *:${env.PORT_SAMPLE_SERVICES}**.
- Right-click, and select **Edit** to display the **Configure HTTP Interface** dialog.



- Modify the **Address** field to change it from '*' to the address of your inbound interface (200.0.0.10



- Click **OK** to save the changes and deploy from Policy Studio.

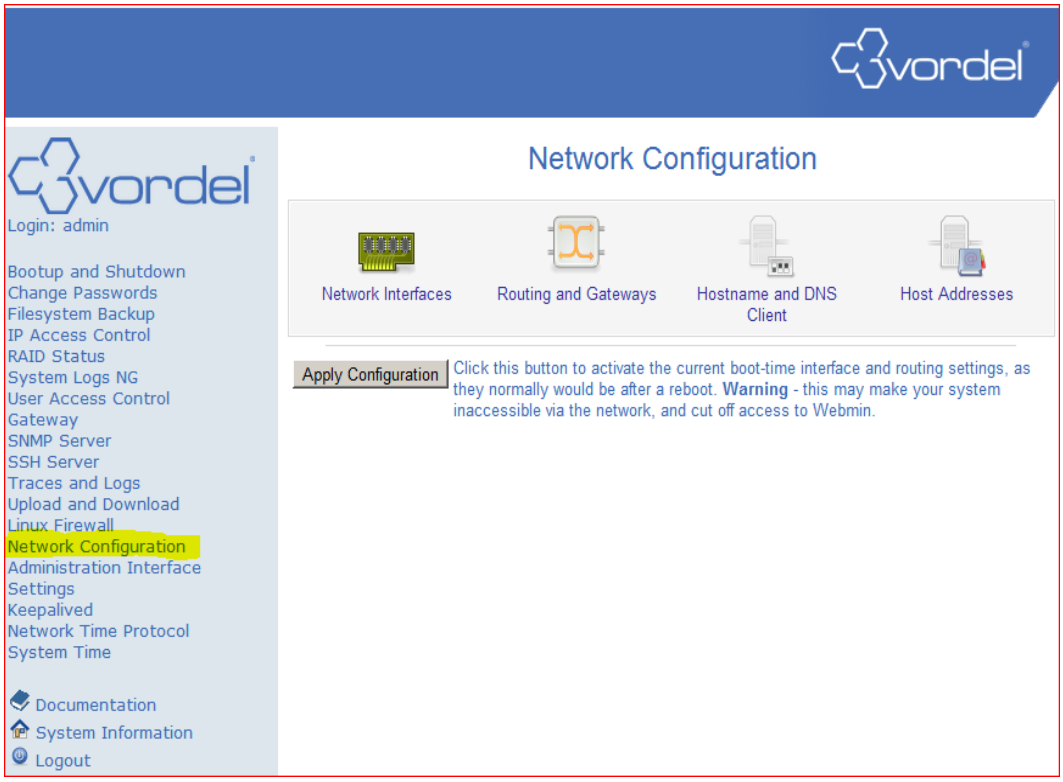
Network Configuration through CLI

The WAI provides an easy to use layer which manipulates the system network scripts. For the Appliance these scripts are located under /etc/sysconfig/network-scripts/ifcfg-<device-name>.

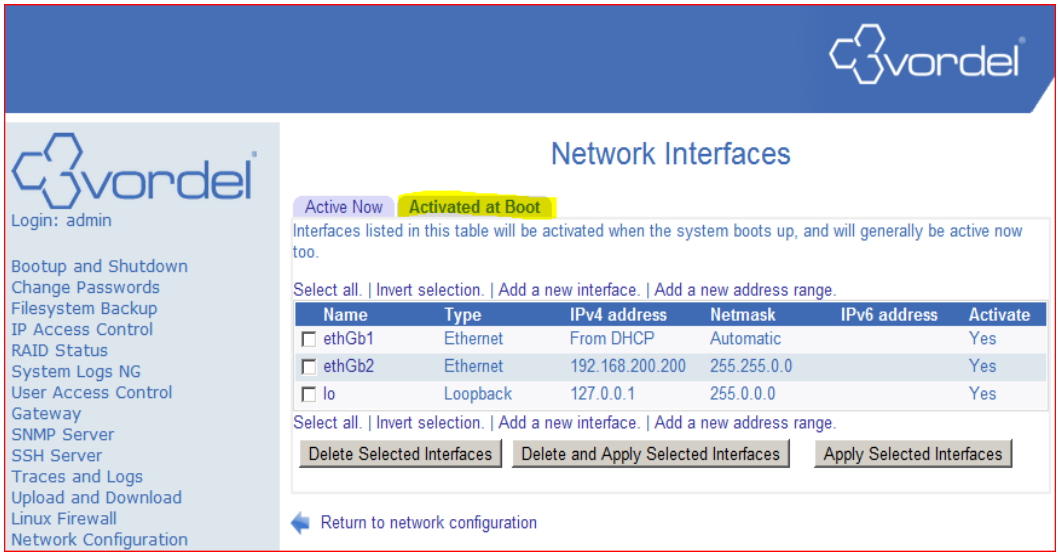
For a user familiar with the layout of these files it is possible to modify the network configuration directly using a root user. Note that any changes made to these files will also be reflected in the WAI

Adding a Virtual IP Address

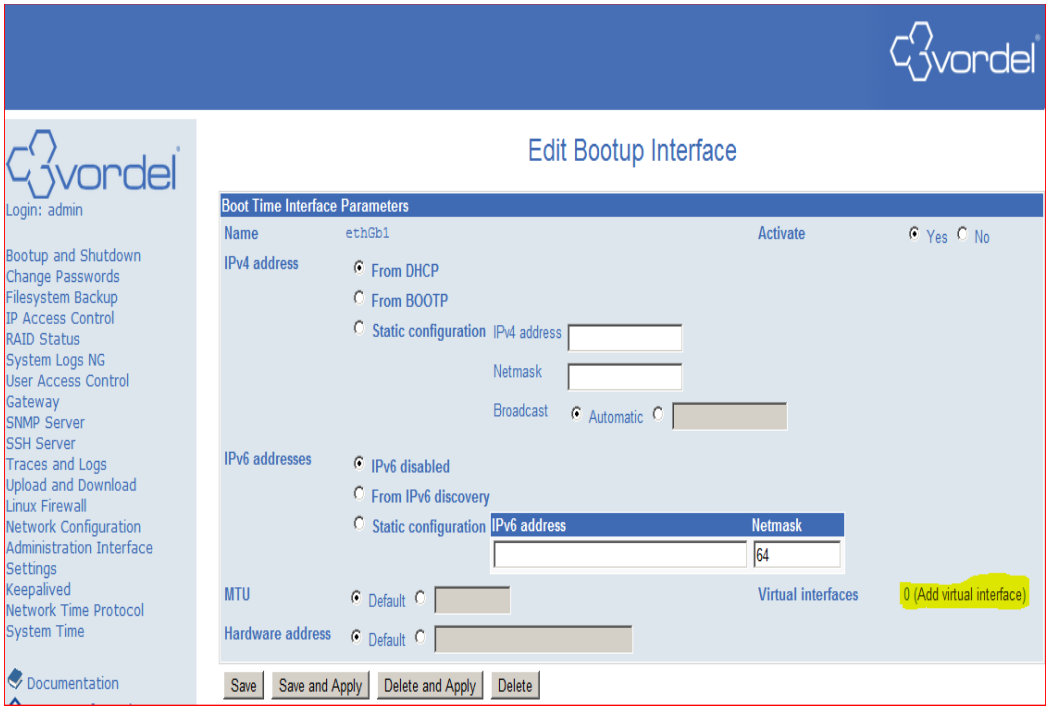
Select the “Network Configuration” menu



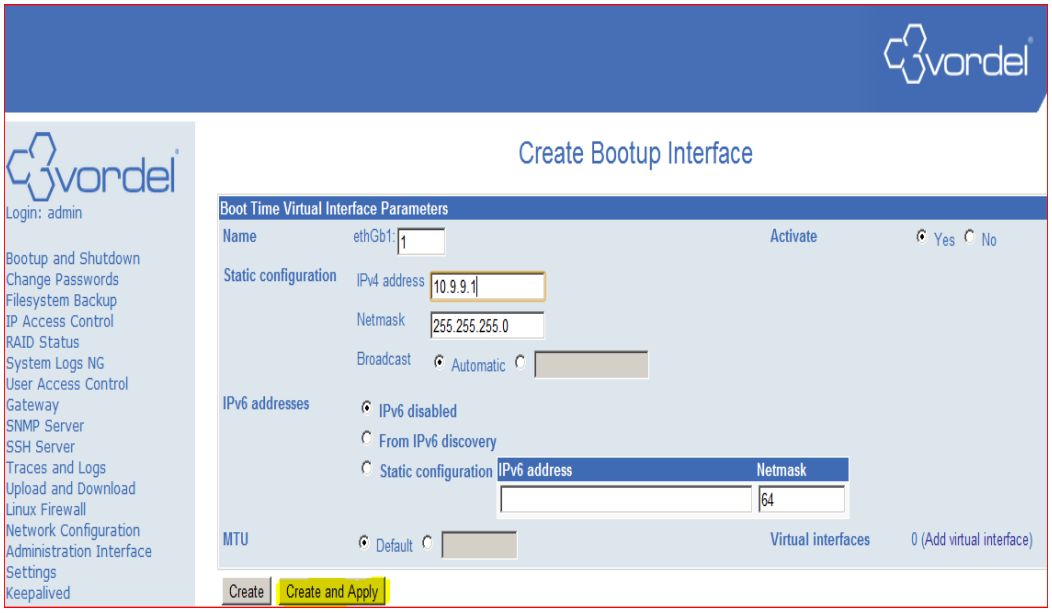
Make sure you click on the “Activated at Boot” tab
Choose an Interface that you want to add a virtual interface too.
For this example we click on ethGb1.



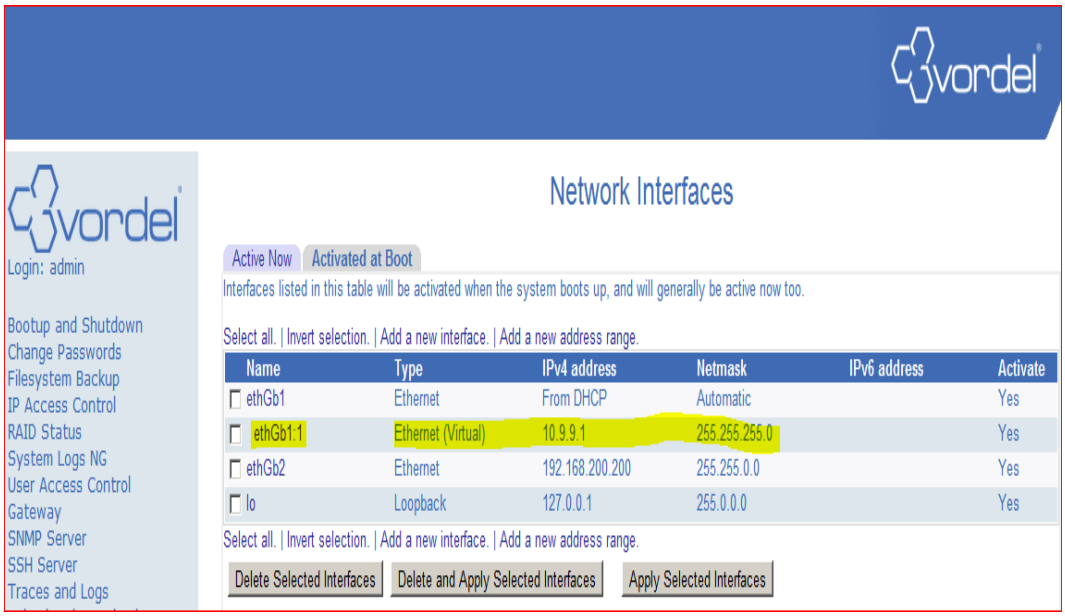
Click on the Add Virtual interface label in the bottom right corner.



Configure the new Virtual Interface settings



Verify that the new Virtual IP has been configured



Check Interface at OS level

```
# ifconfig ethGb1:1
ethGb1:1  Link encap:Ethernet  HWaddr 00:0C:29:28:53:E9
          inet addr:10.9.9.1  Bcast:10.9.9.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Adding Virtual Ip using Command line

Configure Additional IP Addresses

Let's assume our network interface is ethGb1. Then there is a file /etc/sysconfig/network-scripts/ifcfg-ethGb1 which looks like this:

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethGb1
DEVICE=ethGb1
BOOTPROTO=static
BROADCAST=192.168.0.255
HWADDR=00:0C:29:C8:AA:7C
IPADDR=192.168.0.180
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
TYPE=Ethernet
```

Now we want to create the virtual interface `ethGb1:0` with the IP address 192.168.0.101. All we have to do is to create the file `/etc/sysconfig/network-scripts/ifcfg-ethGb1:0` which looks like this (we can leave out the HWADDR line as it is the same physical network card):

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethGb1:0
DEVICE=ethGb1:0
BOOTPROTO=static
BROADCAST=192.168.0.255
IPADDR=192.168.0.101
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
TYPE=Ethernet
```

Afterwards we have to restart the network:

```
# service network restart
```

Adding a Persistent Static Route

It is possible to add a static route with commands similar to
route add -net .. ..

However, static routes added in this fashion will be cleared if the machine is rebooted.

To have static routes persist across reboots you must add a file
`/etc/sysconfig/network-scripts/route-<network-interface>`

The name of the file will correspond to the device which you which to configure the static routes for.
So to configure routes for `ethGb1` the file will be named

```
/etc/sysconfig/network-scripts/route-ethGb1
```

So to configure routes for `ethGb2` the file will be named
```
/etc/sysconfig/network-scripts/route-ethGb2
```

A route added with the following command
```
# route add -net 10.0.7.0 netmask 255.255.255.0 gw 192.168.0.9
```

can be configured persistently with the following file

```
GATEWAY0=192.168.0.9
NETMASK0=255.255.255.0
ADDRESS0=10.0.7.0
```

A second route on the same interface could be configured by adding extra lines to the file like:

```
GATEWAY1=.........
NETMASK1=.........
ADDRESS1=.........
```

To activate the routes, save the file and run:
```
# service network restart
```

Keepalived

Description

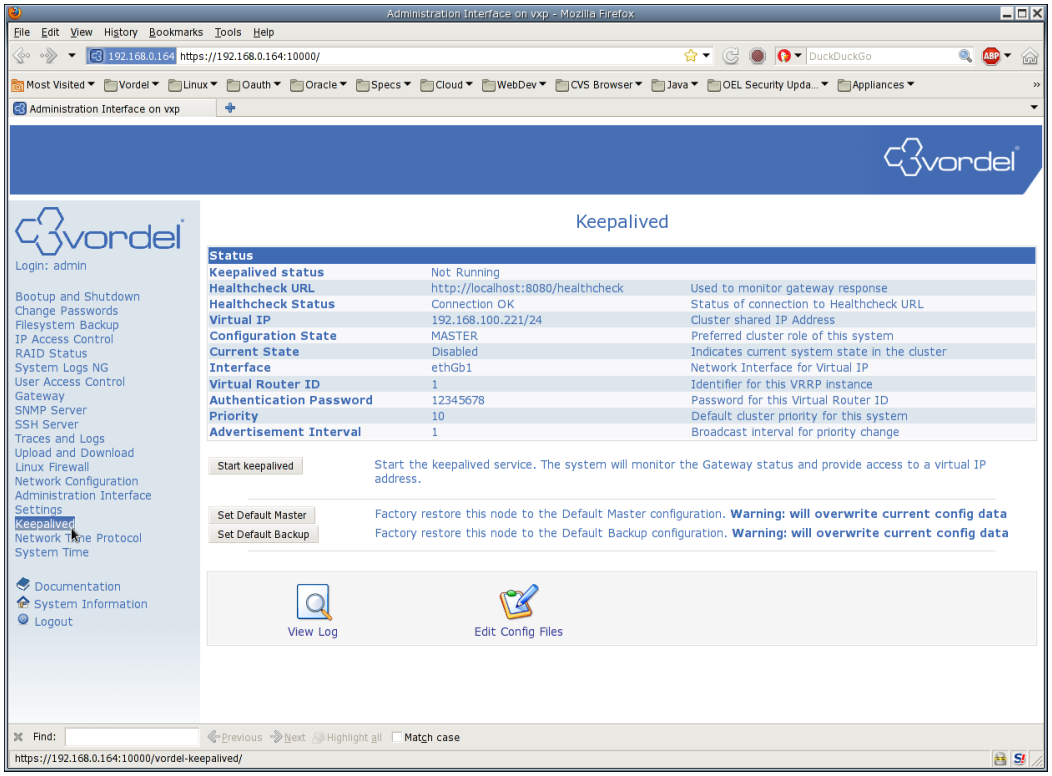
Keepalived is a userspace daemon which provides health checks and failover for cluster nodes in a server pool. It implements a VRRPv2 stack to handle failover, and provides a virtual IP address for the server pool.

The use case from the Appliance perspective is to ensure that the Gateway is reachable on a given IP address, even if one of the servers in a cluster - or Gateway process on one of the servers - fails.

It is possible to configure multiple servers in a cluster, but only one of the servers will be active and listening on the Virtual IP address at a given time. There is no load balancing among the servers in a cluster.

Configuration

The easiest way to configure a cluster and get keepalived up and running is to use the Web Administration Interface. Through the “keepalived” module it is possible to see a status of the keepalived process (whether it is running or not) and some key information about the current keepalived configuration.



The keepalived process can be started, stopped or reloaded from this page and any log messages related to the process can be viewed.

It is possible to edit the configuration file through this module and in addition a stored “Master” or “Backup” style configuration can be loaded on the server.

Quick Start Guide

Following are the steps required to configure a two server cluster using the WAI keepalived module. For the purposes of the example it is assumed that the IP addresses are as follows:

Server1 ethGb1 IP address	**192.168.0.10**
Server1 ethGb1 IP address	**192.168.0.20**
Cluster Virtual IP address	**192.168.0.100**

So if a user wished to connect directly to the gateway running on Server1, they could access a URL similar to http://192.168.0.10:8080/healthcheck

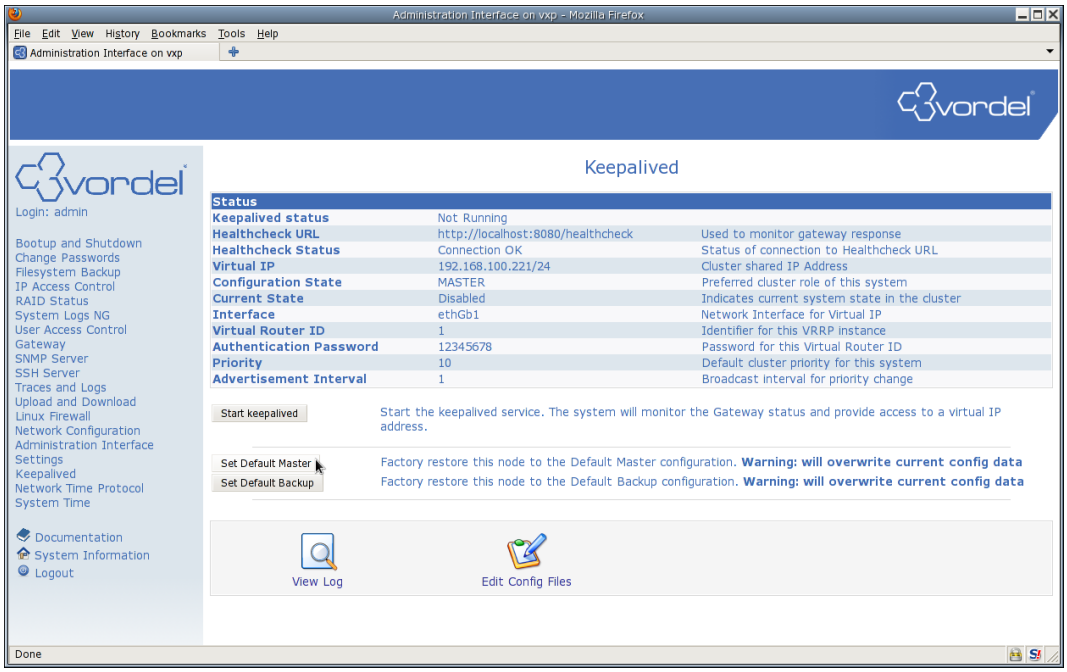
Similarly for Server2 they could access a URL similar to http://192.168.0.20:8080/healthcheck

When the keepalived service is active it will be possible to access a URL similar to http://192.168.0.100:8080/healthcheck

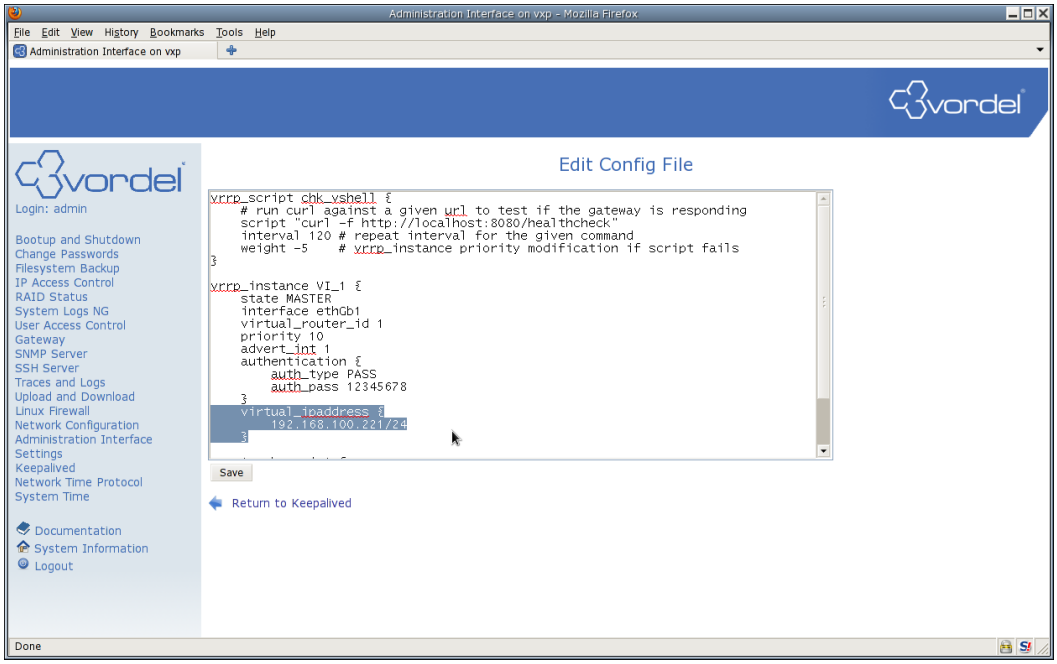
which will be served by either Server1 or Server2.

The steps are:

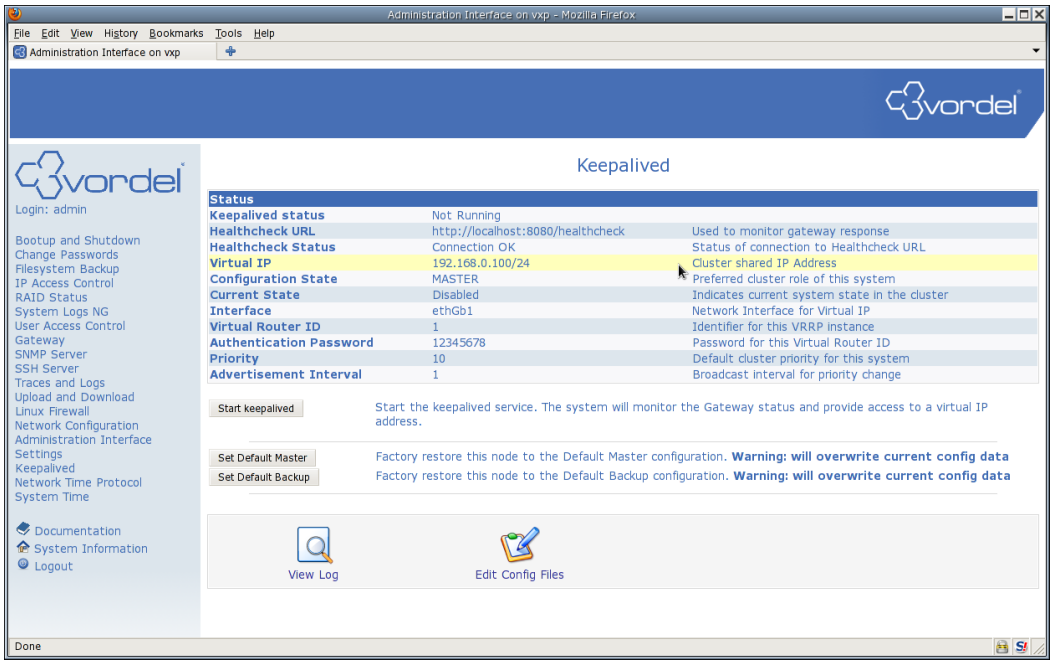
- Log in to the WAI on Server1 using the URL https://192.168.0.10:10000/. This system is going to be configured as the Master or highest priority system in the cluster.
- Click on the “keepalived” link on the left. Here you can see the status of the cluster with details such as the Virtual IP, the Healthcheck status, and whether this server is currently serving on the Virtual IP
- As this system is going to be the Master, click on the “Set Default Master” button. This sets some useful defaults in the configuration such as the priority of this server. After confirmation that the configuration has changed, clicking on the “Return to Keepalived” link



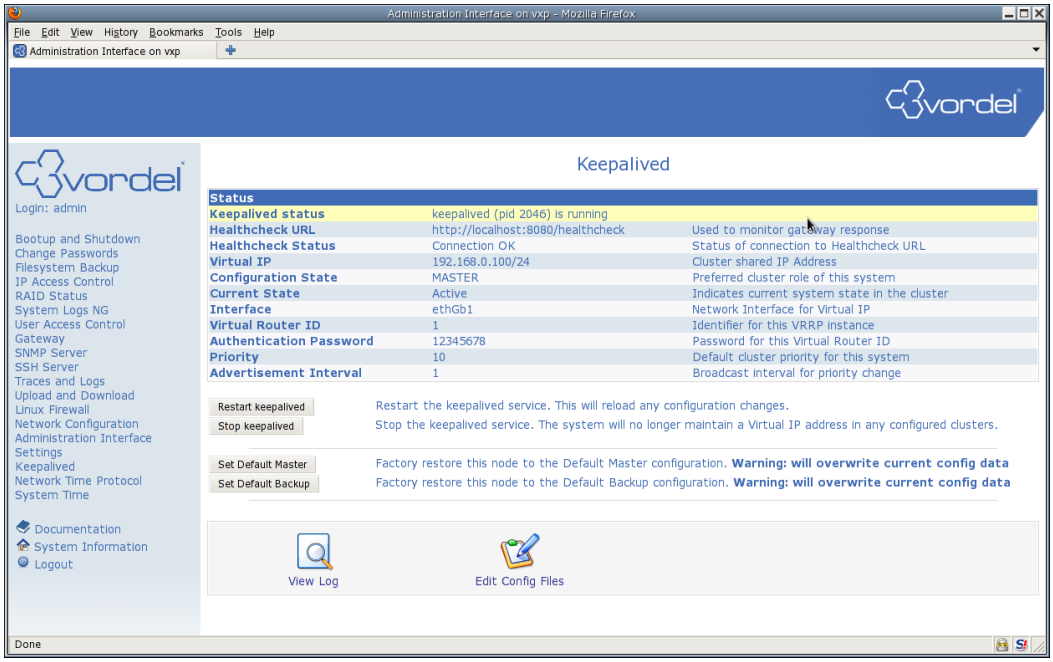
- Some of the defaults in the configuration file will need to be changed so click on the “Edit Config Files” Icon at the bottom of the keepalived page.
- On the Edit Config File page, change the “virtual_ipaddress” section to 192.168.0.100/24 (or whatever IP address you have chosen). Note that the address is given in CIDR format, with the subnet mask given as /24 in this case. Click the “Save” button to change the config.



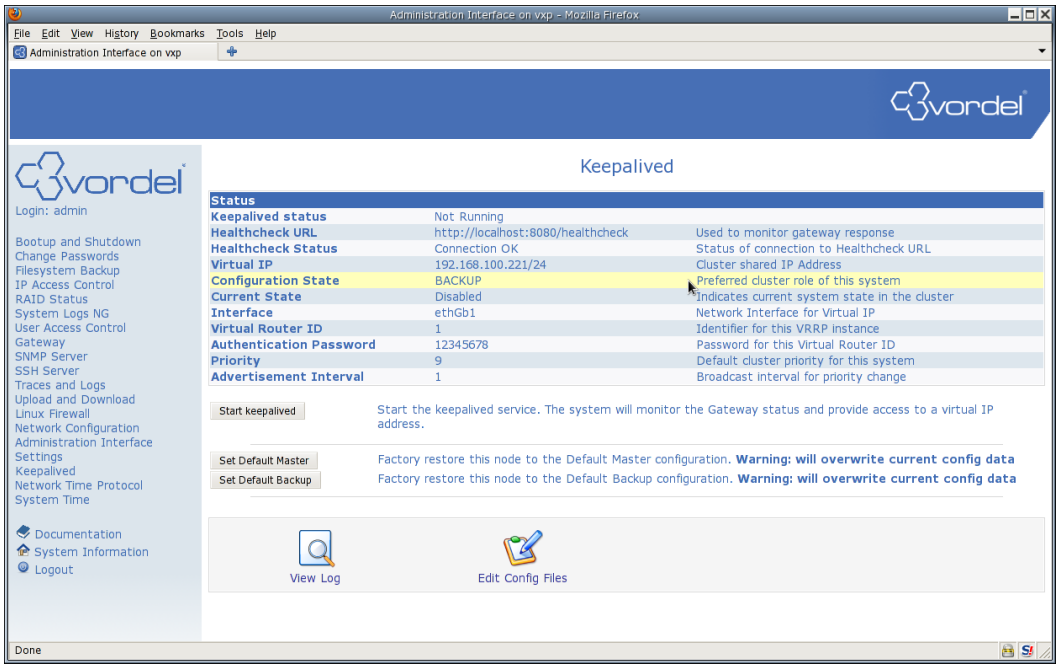
- On the status table you should now see the new IP address in the Virtual IP row.



- If the gateway is currently running you should also see that the Healtcheck Status is OK.
- Click the “Start keepalived” button
- In the status table on this system you should see that the “Configuration State” is MASTER and the “Current State” is “Active”.

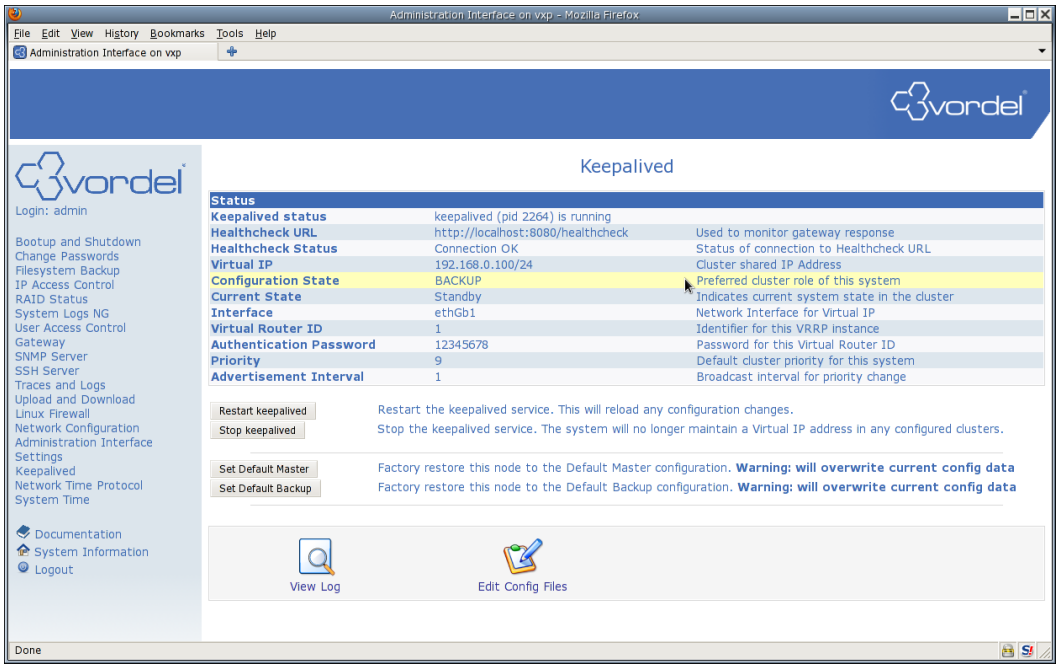


- Now log in to the WAI on Server2 using the URL https://192.168.0.20:10000/.. This system will be configured as the Backup system. If there is an issue on Server1, this system will be promoted to Master state, and will server requests on the Virtual IP address.
- Click on the “keepalived” link on the left.
- As this system is going to be the a Backup, click on the “Set Default Backup” button. After confirmation that the configuration has changed, clicking on the “Return to Keepalived” link



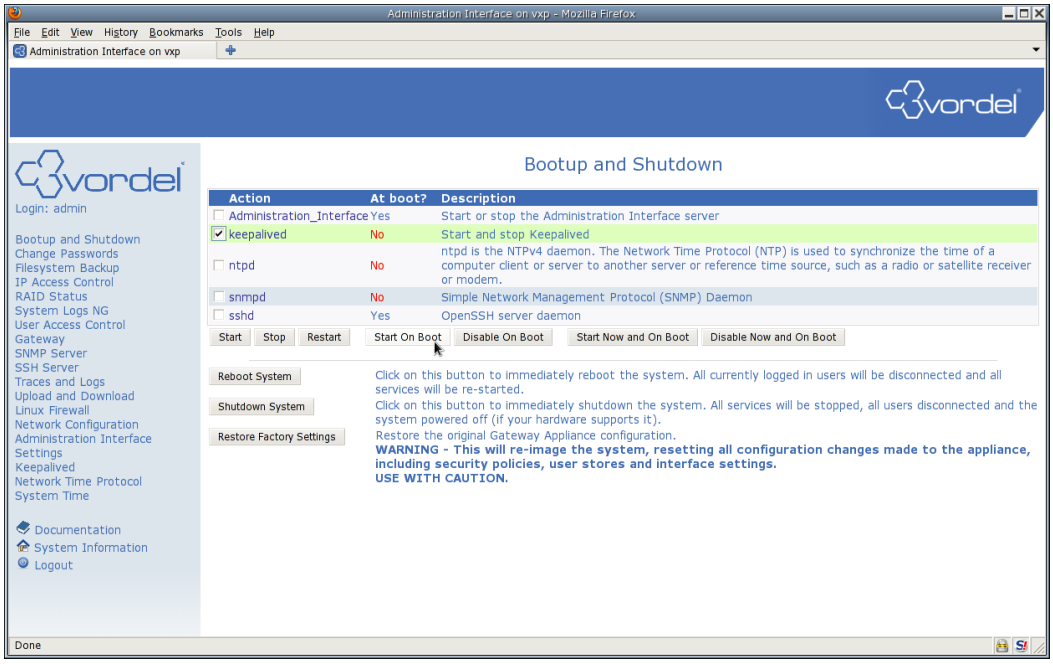
- Some of the defaults in the configuration file will need to be changed so click on the “Edit Config Files” Icon at the bottom of the keepalived page.
- On the Edit Config File page, change the “virtual_ipaddress” section to 192.168.0.100/24 (or whatever IP address you have chosen). Note that the address is given in CIDR format, with the subnet mask given as /24 in this case. Click the “Save” button to change the config.

- On the status table you should now see the new IP address in the Virtual IP row.
- If the gateway is currently running you should also see that the Healthcheck Status is OK.
- Click the “Start keepalived” button
- In the status table on this system you should see that the “Configuration State” is Backup and the “Current State” is “Standby”.



- Attempt to connect to a URL using the virtual IP address and it should work as expected.

Note that the keepalived service is disabled by default on the Appliance. If you wish the service to start automatically on system bootup then you must change the default in the “Bootup and Shutdown” section. Select “keepalived” and click the “Start on Boot” button.



By default keepalived performs a healthcheck on the gateway every 120 seconds. To change this to a lower value edit the “interval” value in the “chk_vshell” section of the configuration file.

Multiple clusters on same network

If you wish to have more than one discrete cluster running on the same network then you will have to modify the default configuration. The settings which need to be changed are:

- virtual_router_id
- auth_pass

For each cluster you will need a unique value for these variables. Each system in that cluster will need the same value in it’s configuration file.

Firewall

For keepalived to work you need to allow access through the firewall for packets with a destination of 224.0.0.18 and protocol 112 (VRRP). This is set up on the Appliance version 6.3.1 and greater by default.

Debugging

To debug keepalived check /var/log/messages for any errors.
Common problems arise from having incorrect or non-matching entries in the configuration files. Double check the values of virtual_router_id, virtual_ipaddress, auth_pass and priority.
Also check that it is possible to reach the Healthcheck URL. This is given on the keepalived status page but you could also log into the Appliance directly and run the curl command against the URL.

To check the keepalived traffic reaching the system run the following tcpdump command (when logged in as root to the Appliance):

```
# tcpdump -envi ethGb1 host 224.0.0.18
```

This should show you packets between different hosts in the cluster. If there is no traffic coming through then check the firewall on any systems in the cluster and also check the status of the service.

Configure Keepalived to send email on State Change

It is possible to configure keepalived to send email notifications of state changes, i.e. when a system changes from a Master to Backup state or vice versa. Some changes to the configuration must be made and sendmail must be enabled, if using the Appliance as the mailserver.

Instructions are as follows.

Enabling sendmail on the Appliance

The sendmail daemon is installed but disabled by default on the Appliance. Before the Appliance can send emails from keepalived you must start the sendmail service.

Log in as root to the Appliance and carry out the following commands

```
# service sendmail start
```

And to enable the sendmail service automatically at boot time run

```
# chkconfig sendmail on
```

Enabling email notification in Keepalived config

The following section must be added to the keepalived config file on both systems. Note that most details in these sample config files will need to be modified to suit your environment.

```
global_defs {
   # addresses here are destinations for emails from the server
   notification_email {
        example_user1@example.com
       example_user2@example.com
   }

   # For clarity it is suggested that the from address
   # given here is different on each server in the cluster
   notification_email_from root@APIAppliance.com

  smtp_server 127.0.0.1
   smtp_connect_timeout 30
   # System identifier for subject of email
   router_id Appliance_hostname-or-IP_address
}
```

It is strongly recommended that the the `router_id` and `notification_email_from` sections are unique for each server in a cluster.

In the `vrrp_instance` section of the config file the line `smtp_alert` must also be added.

```
vrrp_instance VI_1 {
    state MASTER
    interface ethGb1
    virtual_router_id 5
    priority 10
    advert_int 1
    smtp_alert
    authentication {
        auth_type PASS
        auth_pass 12345678
    }
    virtual_ipaddress {
        192.168.0.241/24
    }

    track_script {
        chk_vshell
    }
}
```

You must restart keepalived to load the configuration changes.

```
# service keepalived restart
```

Updating Software

Introduction to yum

Yum is a tool which provides a way to easily manage RPM software packages and their dependencies on a system. When using yum to update software it will check configured package repositories to find latest versions of RPMs and any dependencies required to install updates.

The kingsofsoa yum repository

Axway maintains a repository which contains updates to packages along with any security updates to Appliance specific OS packages. It is already included in the Appliance distribution and can be reached at http://www.kingsofsoa.vordel.com/vordel

Applying Security Updates

To check if any new versions of the system packages are available run the following command:

```
# yum check-update
```

This will return a list a of packages from the kingsofsoa-vordell repository if there are updates required.

Running the command:

```
# yum update -y
```

will install the new packages.

It is recommended that the “check-update” command is run when the system is first deployed, and periodically afterwards.

Updates on System without Internet Access

If the system to be updated does not have access to the Internet then it will not be possible to use yum for any updates. In this case support will be able to provide a list of packages required for your system. To do this it will be necessary to provide support with a list of the currently installed packages.
Run the following command:
`# rpm -qa > installed_rpms.txt`
and provide the file *installed_rpms.txt* to Support.

They will then give you a list of RPMs which you will need to copy to the system which is to be upgraded. Change directory to the location where these new RPMs have been copied and execute:
`# rpm -Uvh *.rpm`

This will update the necessary packages.

Creating a Local Clone of the Yum Repo

See the following doc:
https://docs.google.com/a/vordel.com/document/d/1a_aHMt7Fy7wkdZveA-gu7v2eZBaOj3bvvyJwsxcamh4/edit#heading=h.2a2ykl5iqslc

Using Yum Through a Proxy Server

To enable all yum operations to use a proxy server, specify the proxy server details in `/etc/yum.conf`. The proxy setting must specify the proxy server as a complete URL, including the TCP port number. If your proxy server requires a username and password, specify these by adding `proxy_username` and `proxy_password` settings.

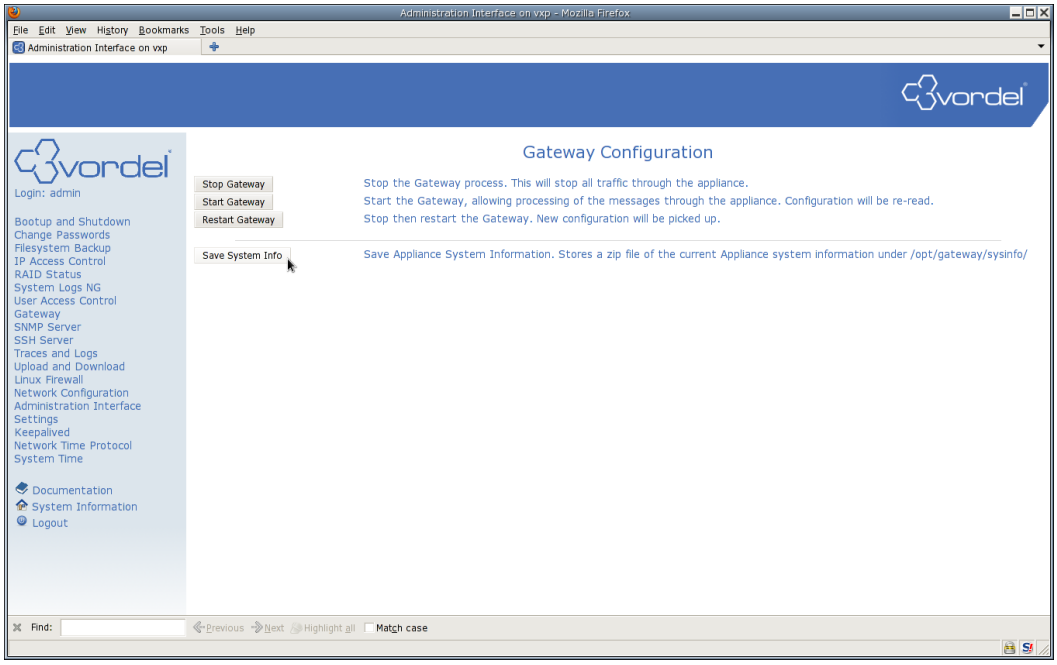
The settings below enable yum to use the proxy server `mycache.mydomain.com`, connecting to port `3128`, with the username `yum-user` and the password `qwerty`. These lines would be added to `/etc/yum.conf`

```
# The proxy server - proxy server:port number
proxy=http://mycache.mydomain.com:3128
# The account details for yum connections
proxy_username=yum-user
proxy_password=qwerty
```

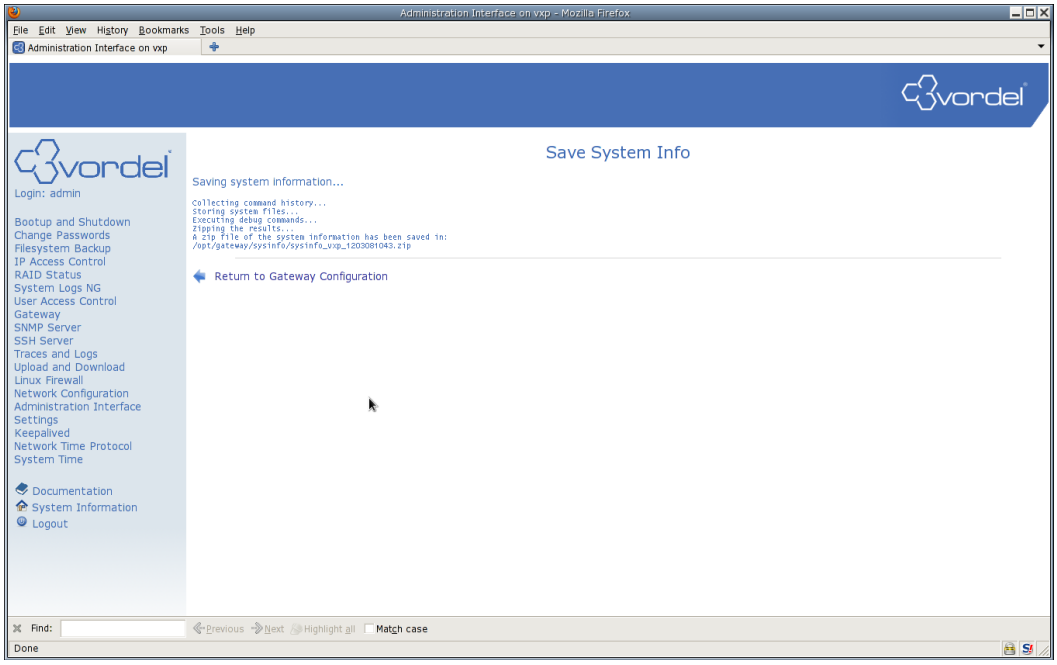
Providing System Information to Support

If there is any issue with your system it is very important and as much information about the configuration of the the system is provided to support so that they can provide the correct help that you need.
To this end there is a simple command which can be run on the Appliance which will execute a number of debug commands and collect the results in a zip file. This zip file can then be copied from the system and provided to support.

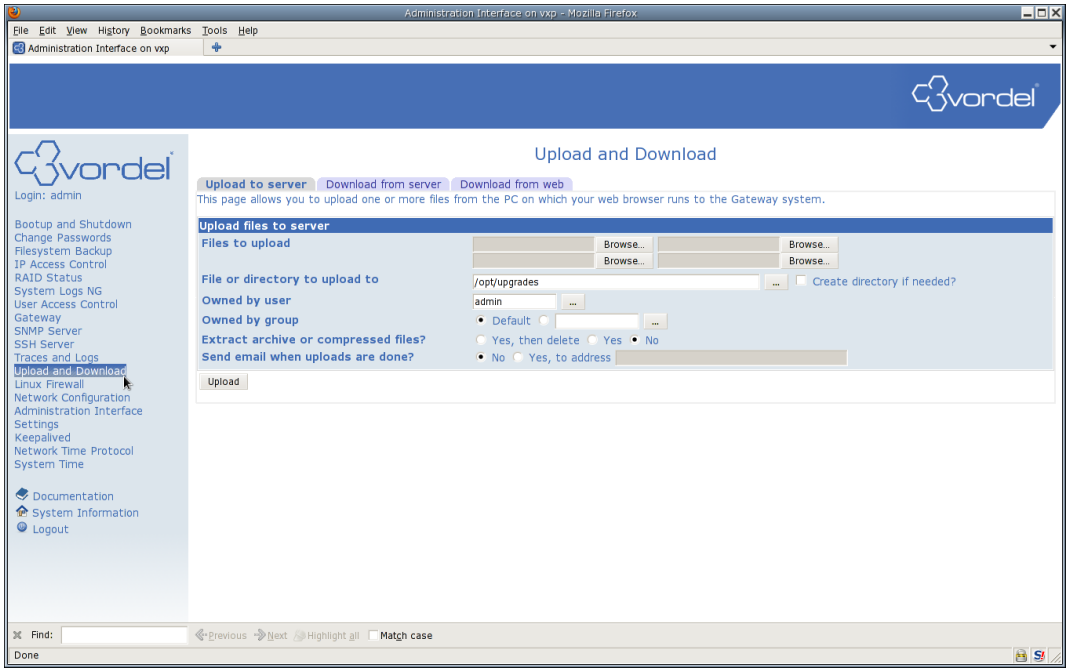
To execute the command log in to the WAI and select the Gateway menu item. Click on the button to Save System Info



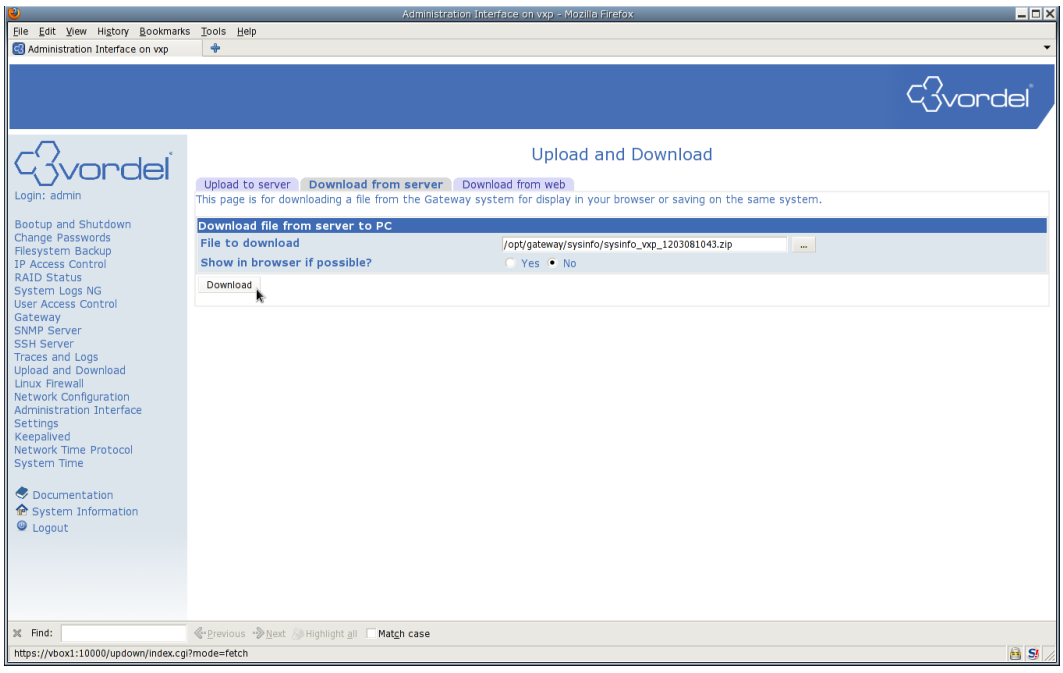
This command may take a few minutes to complete but the output should be similar to



Make a note of the output name of the zip file. This can then be downloaded from the system through the “Upload and Download” screen. Click the “Upload and Download” link on the left.



Then click the “Download from Server” tab and enter the full filename for the zip file created by Save System Info. Click the “Download” button and the file can be saved locally.



This file should then be sent to support.

SNMP

An SNMP server runs on port 161 on the appliance to allow an NMS (Network Management System) to query status information from the appliance. The SNMP server can be configured to run on any of the interfaces on the appliance. To configure the SNMP server, click the **SNMP Server** link in the WAI.

Complete the following fields on this page:

1. In the **System Details** section, enter the location of the host on which the SNMP agent runs in the **Location** field and the system contact address in the **Contact** field. Click the **Save Details** button to record the system details.

2. If you wish to allow SNMP version 1 or 2c clients to connect to the SNMP server, you must configure a set of SNMP *communities* in the **SNMP V1/V2c Communities** section. Most of the configuration settings for existing communities can be edited directly using the fields in the **SNMP V1/V2c Communities table**. If you change any settings in the table, you must click the **Apply Changes** button to finalize the changes. A new community can be added by clicking on the **Add New Community** button and complete the following fields:

2.1. Enter the unique name of the community in the **Name** field.

2.2. The network address specified in the **IP/Netmask** field dictates the network from which members of the specified community can access the SNMP server. The network address is specified using CIDR-style notation, which consists of the dotted IP address of the network followed by a '/' and then a prefix length. For example, in comparison to traditional netmask usage, 192.168.0.0/24 indicates the 192.168.0.0 network with a netmask of 255.255.255.0.

2.3. Members of the community on the selected network can be assigned either 'Read Only' or 'Read/Write' permissions and can also be disabled using the **'Permissions'** dropdown.

2.4. Click on the **Create new Community** button to finalize the changes.

2.5. And finally, the community can be deleted by selecting the **Delete** checkbox on the main **SNMP Server Configuration** page and clicking the **Apply Changes** button. Note that a default community named 'public' has been pre-configured on the appliance to grant 'Read Only' permissions to clients from any network (i.e. it has a netmask of 0.0.0.0/0).

3. If you would like SNMP version 3 clients to be able to connect to the SNMP server, you must specify the SNMP *users* in the **SNMP V3 Users** section. The configuration settings for existing users are displayed in the **SNMP V3 Users** table. It is possible to edit a user's details directly by modifying the values in the table and then clicking the **Apply Changes** button. For example, users can be disabled by selecting the 'Disabled' option from the **Permissions** dropdown or deleted using the **Deleted** checkbox, followed by clicking the **Apply Changes** button. To add a new user click the **Add New User** button and complete the following fields:

3.1. Enter a name for the new user in the **Name** field.

3.2. Specify the permissions for the new user using the **Permissions** dropdown. It is possible to configure 'Read Only' or 'Read/Write' permissions. You can also disable a user by selecting the 'Disable' option. Note that if you wish to *only* change the user's permissions, make sure to select the 'Retain password' option from both the **'Authentication Algorithm'** and **'Privacy Algorithm'** dropdowns.

3.3. Select the algorithm to use when hashing the user's password by selecting either 'MD5' or 'SHA' from the **'Authentication Algorithm'** dropdown.

3.4. Enter the user's password in the **Authentication Password** field. It is important to note that if either the password or algorithm is changed for an existing user, the **'Privacy Algorithm'** and **'Privacy Password'** must also be changed/re-entered.

3.5. Select either 'DES' or 'AES' from the **'Privacy Algorithm'** dropdown. The selected algorithm will be used to encrypt the channel between the SNMP client and server.

3.6. Enter the password to use to encrypt and decrypt data sent to/from the client in the **'Privacy Password'** field. Please note that if you change either the password or algorithm for an existing user here, the **'Authentication Algorithm'** and **'Authentication Password'** must also be changed/re-entered.

3.7. Click the **'Create New User'** button to create the new user.

4. In the **'Networking Options'** section, enter the IP addresses of the interfaces that you want the SNMP server to run on in the **'Listen on Addresses'** fields. Click the **'Save Settings'** button when you have entered the relevant addresses.

5. The **MIBs** link can be used to view the MIBs (Management Information Bases) that are understood by this machine. An NMS will use the same MIBs installed on the appliance to make sense of the status information retrieved from the machine, e.g. interpret object identifiers, etc. A file listing of MIB files installed on the appliance will be displayed in a new window. It is possible to view any of the MIB files by clicking on the filename. The MIB can then be saved from your browser and then imported into an NMS.

Allowing SNMP connections

As a security measure, the XML Gateway appliance comes with SNMP daemon configured to listen only on loopback interface of the appliance and thus is inaccessible from the network. Therefore, in order to use SNMP monitoring, you must firstly enable the SNMP interface.
To allow external connections to SNMP daemon please follow these steps:

1. Connect to the Web Administrative interface of API Gateway appliance.
2. Choose which network interface we will have the SNMP daemon listening on. Go to the following location:
   System -> Network Configuration -> Network Interfaces screen.
   Make a note of the IP address, note it is recommended that this is not the same IP address that is being used for XML traffic
3. Go to the SNMP Server screen.

4. Set ‘Listen on Address’ option of ‘Networking Options’ section to the IP address chosen in step 2.

Automatically Starting SNMP Service

As as security measure the SNMP server daemon is not automatically enabled on the Appliance. To have it start automatically on system bootup you must enable the snmpd service in the WAI Bootup and Shutdown screen.

Syslog

Overview

The System Logs page enables you to control the Syslog-NG daemon running on the appliance, and to view its output.

Logging Options

This page enables you to configure the global behavior of the Syslog-NG daemon. For example, you can configure how hostnames and DNS lookups are handled, and how default permissions are assigned to trace files and the directories where they are stored. However, you can override these global configuration options on a per-destination basis using the Log Destinations configuration screen, as described in this topic.

Log Source

A Log Source enables you to configure several ways that the Syslog-NG daemon can receive log messages, including from a UNIX socket, Linux kernel, or from other systems on the network. The Log Sources page lists all known sources. You can add a new source by clicking the Add a new log source link. You can edit existing sources by clicking the link identifying the source.
In both cases, the Log Source Options page enables you to configure which data source types are used by the Log Source. For example, you can specify whether the Log Source receives messages from a Stream Socket, Datagram Socket, TCP Server, or from a Named Pipe, amongst other types.
When configuring the options for each source type, the default options are typically sufficient for most system configurations.

Log Destinations

All services running on the appliance trace output to the Syslog-NG daemon running on the appliance. You can view this trace output by clicking the Log Destinations page.
Trace files corresponding to the services running on the appliance are listed in a table on this page. To view a particular trace file, click the View link beside that entry in the table. The contents of the selected trace file are displayed on a new page. In cases where the trace file is large, you can select to view only a specified number of lines, and search through the file for lines that only show certain text.

Log Filters

A Log Filter enables you to define a set of conditions that may match a particular log message based on its facility (source program type), priority (severity level), contents, sender's hostname and IP address, and so on. The filter can then be combined with a source and destination in a log target to determine what

log messages are written to the destination.
The Log Filters page lists all existing filters and can be used to create new filters and edit existing ones. You should only edit default filters under advice from the support team because any erroneous configurations may prevent critical log messages being written.
Syslog-NG enables you to use boolean logic to create very complex filters to match messages. However, in most cases, you can use a simple set of rules based on the facility, priority, contents, hostname, and source IP address of the message. You can write a Syslog-NG boolean expression to create more powerful filters.

Log Targets

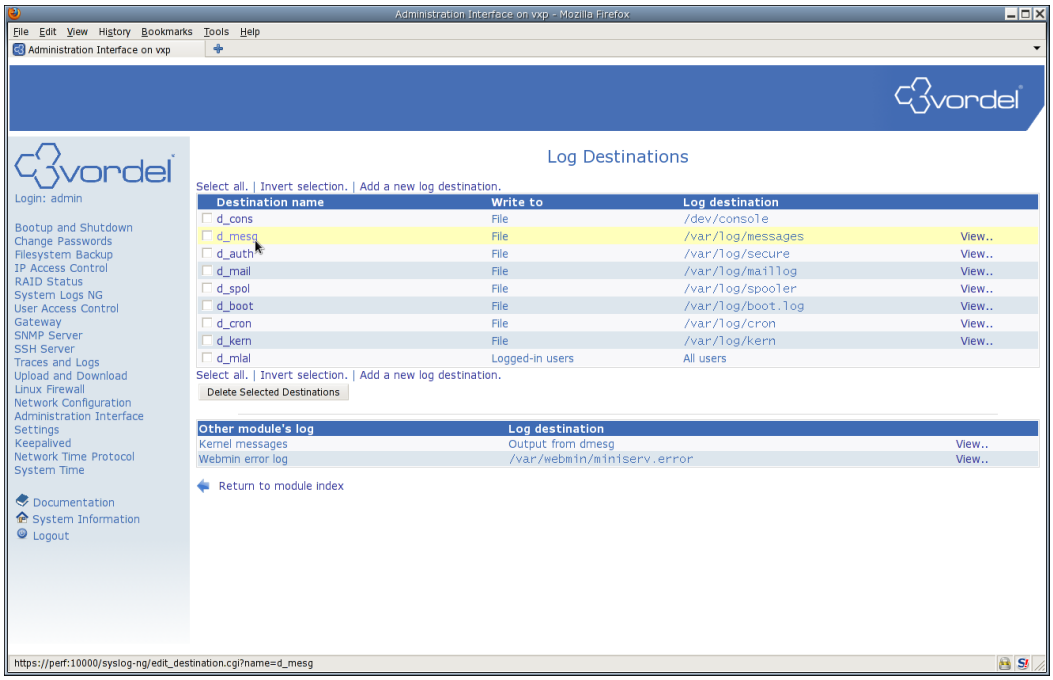
Log Targets are used to bring together sources, destinations, and filters to determine exactly what messages are logged and to where. Each target comprises one or more sources, zero or more filters (to determine what messages are logged), and one or more destinations (to control where to log the messages to).

The Log Targets page lists all existing log targets. You can configure one of these targets by clicking its link. The target can then be configured easily by selecting the source(s), filter(s), and destination(s) from the lists.

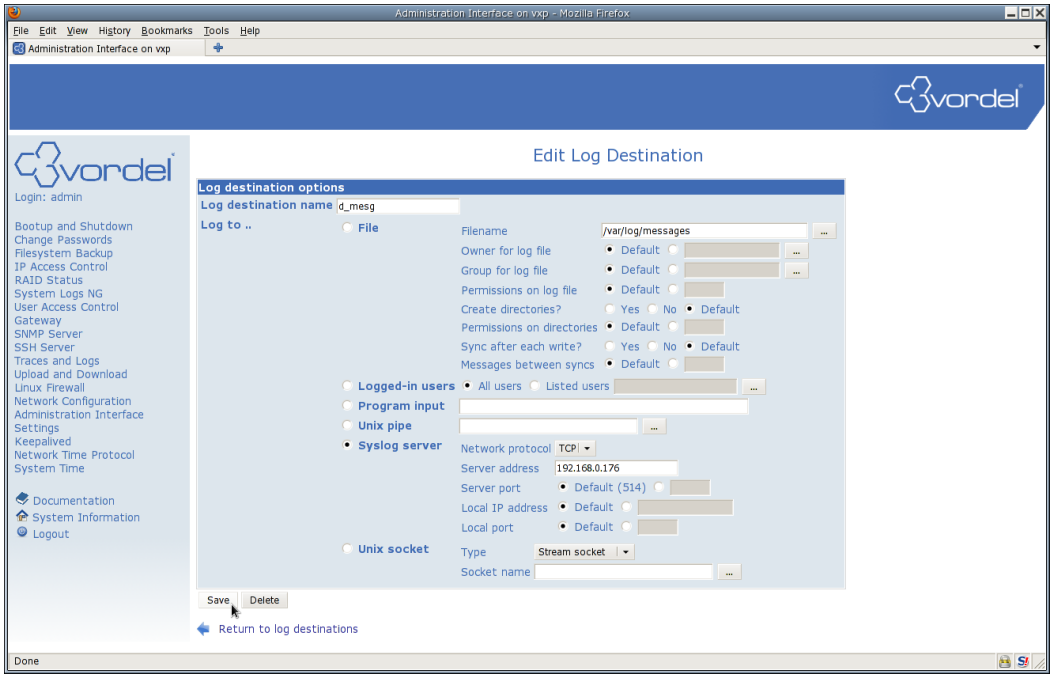
Example configuration for Remote Syslog

To send syslog messages to a remote server you must reconfigure the log destinations through the WAI. In this example we will reroute the messages which would normally be sent to */var/log/messages*.

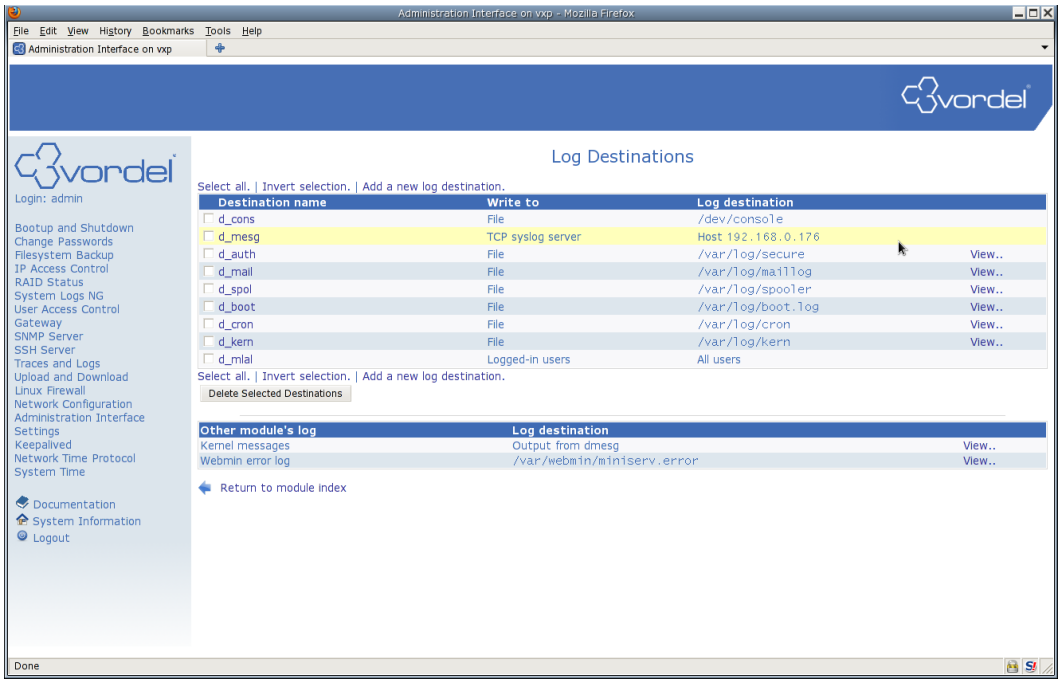
Log in to the WAI, Select System Logs NG and click on the d_mesg destination.



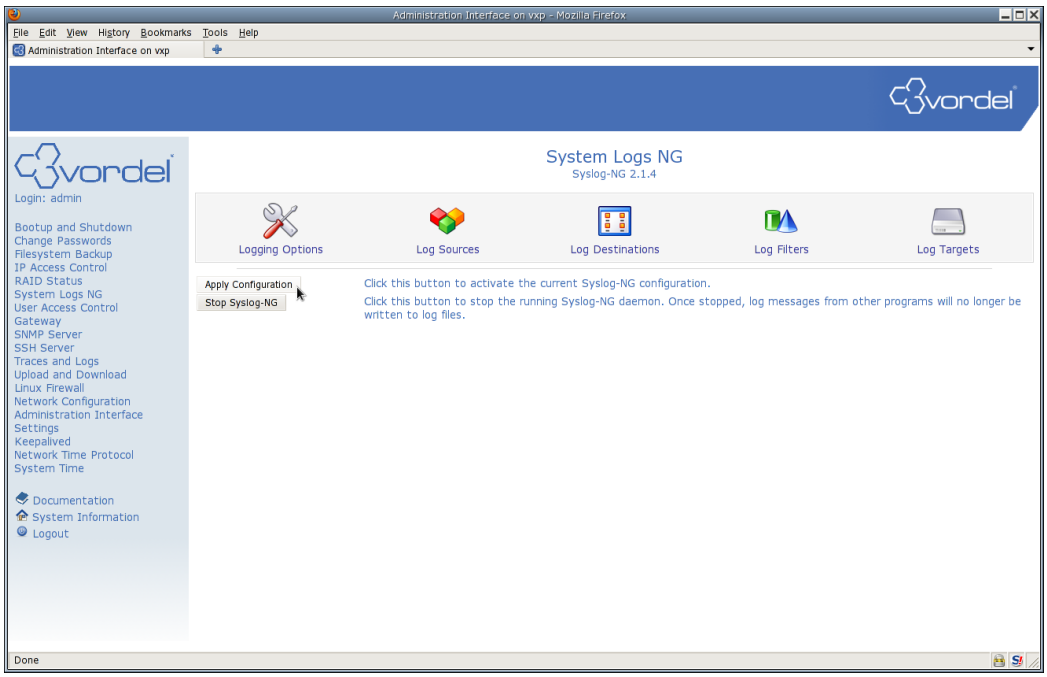
In the Edit Log Destination screen, click the Syslog Server section. Select TCP or UDP communication and a port number. Enter the IP address of the remote syslog server. (If you do not know this information you must contact the administrator of your remote syslog server). Click the Save button.



You will see the updates on the Log Destinations screen. Click “Return to module index”



Now click Apply Configuration to update the syslog-ng process.



Additional Hardware

iDRAC

iDRAC6 is concerned with monitoring and managing the server's environment and state outside of the operating system. The iDRAC assigned IP address is separate to the operating system.

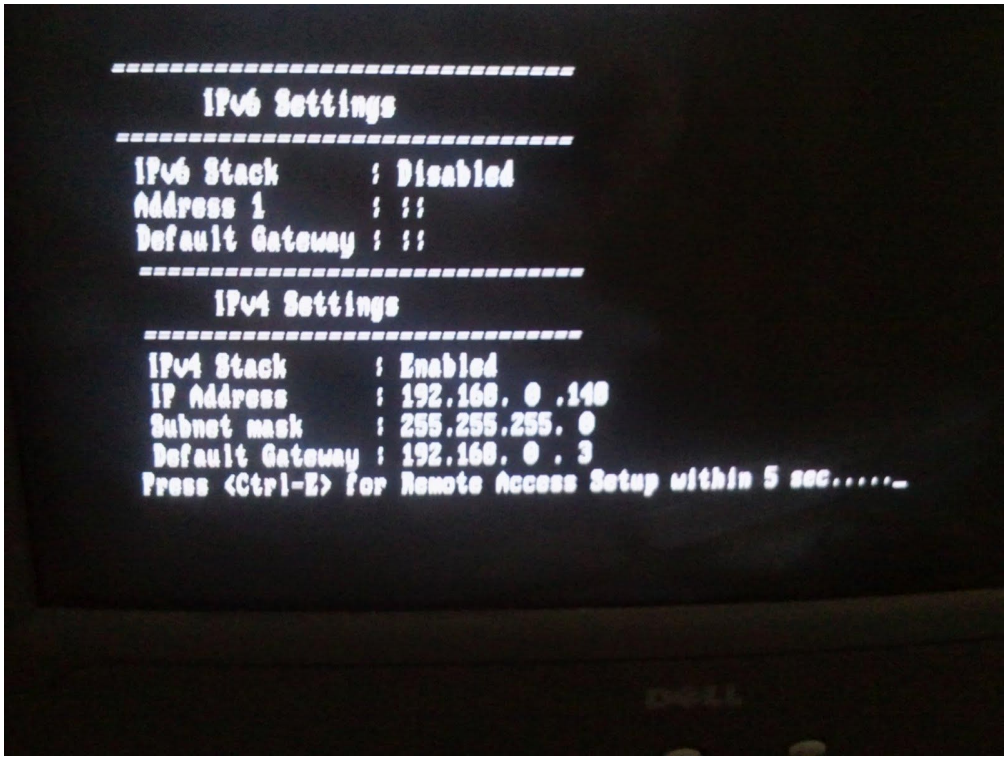
The appliance doesn't ship with a dedicated interface it uses iDRAC express which shares the physical connection of ethGb1 on the onboard NIC.

Configure iDRAC Network Settings

The iDRAC6 network interface is enabled with a static IP address of 192.168.0.120 by default. It must be configured before the iDRAC6 is accessible. After the iDRAC6 is configured on the network, it can be accessed at its assigned IP address with the iDRAC6 Web interface, Telnet, or Secure Shell (SSH), and supported network management protocols, such as Intelligent Platform Management Interface (IPMI).

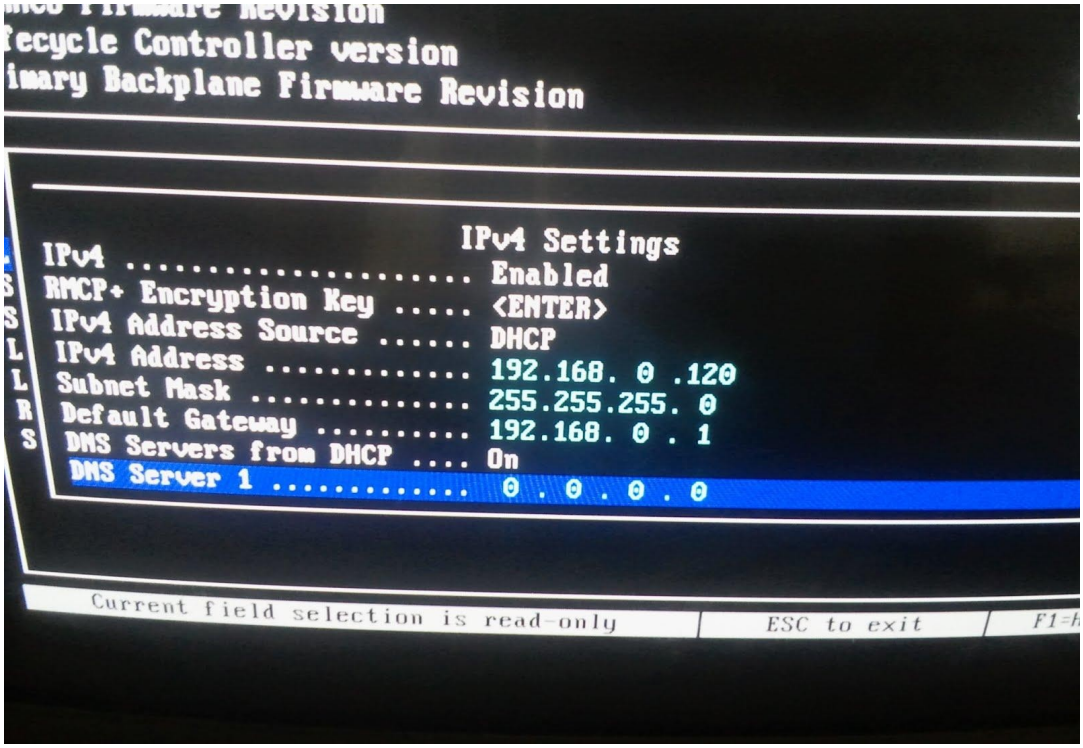
How to configure iDRAC and enable it through DELL BIOS

From BIOS settings, enter *Ctrl - E* for iDRAC setup when prompted.
You can then modify the settings including IP details.

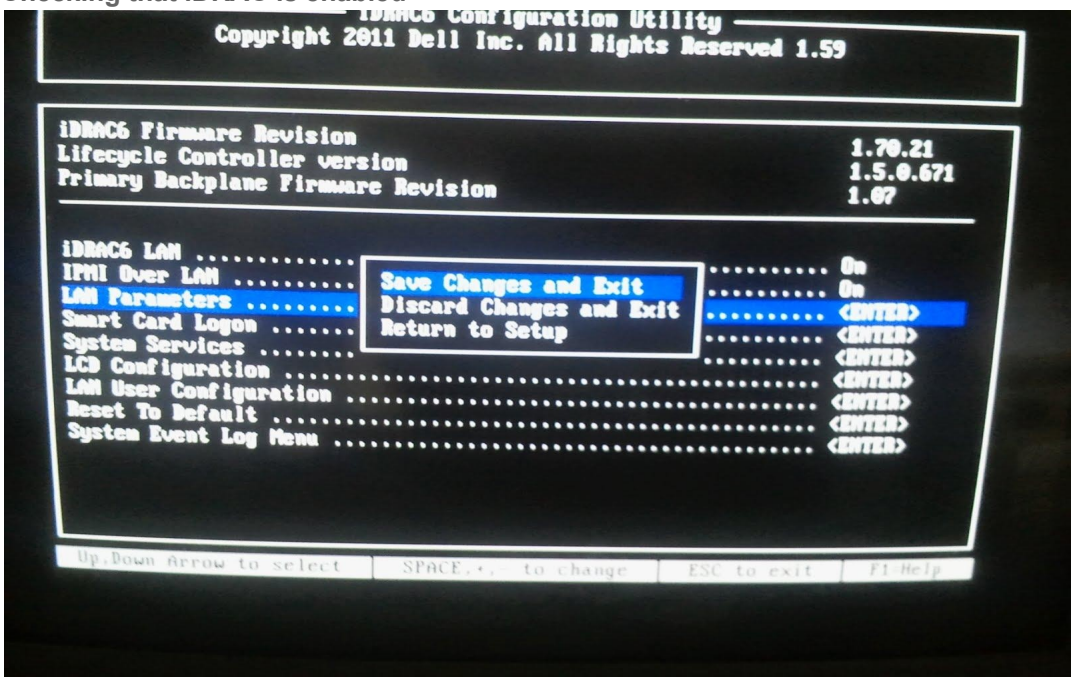


Changing IP Address

After entering *Ctrl-E* you can modify the ip address settings for the iDRAC interface.



Checking that iDRAC is enabled



How to configure iDRAC and enable it through CLI

Check current iDRAC nic settings

[20:09:12]# racadm getniccfg

IPv4 settings:
NIC Enabled = 1
IPv4 Enabled = 1
DHCP Enabled = 1
IP Address = 192.168.0.148
Subnet Mask = 255.255.255.0
Gateway = 192.168.0.3
…...
….
LOM Status:
NIC Selection = Shared
Link Detected = Yes
Speed = 1Gb/s
Duplex Mode = Full Duplex
Active LOM in Shared Mode = NIC1

Manually set iDRAC nic address

racadm setniccfg -s 192.168.0.121 255.255.255.0 192.168.0.3
Static IP configuration enabled and modified successfully

Set iDRAC ipaddress to DHCP

[20:19:08]# racadm setniccfg -d
DHCP is now ENABLED
[root@appliance ~]
[20:19:57]# racadm getniccfg

IPv4 settings:
NIC Enabled = 1
IPv4 Enabled = 1
DHCP Enabled = 1
IP Address = 192.168.0.148
Subnet Mask = 255.255.255.0
Gateway = 192.168.0.3
…..
…..

Testing using a Laptop and CrossOver cable

Laptop Network Config when IDRAC on appliance is in factory default mode.

Set up the laptop or PC:

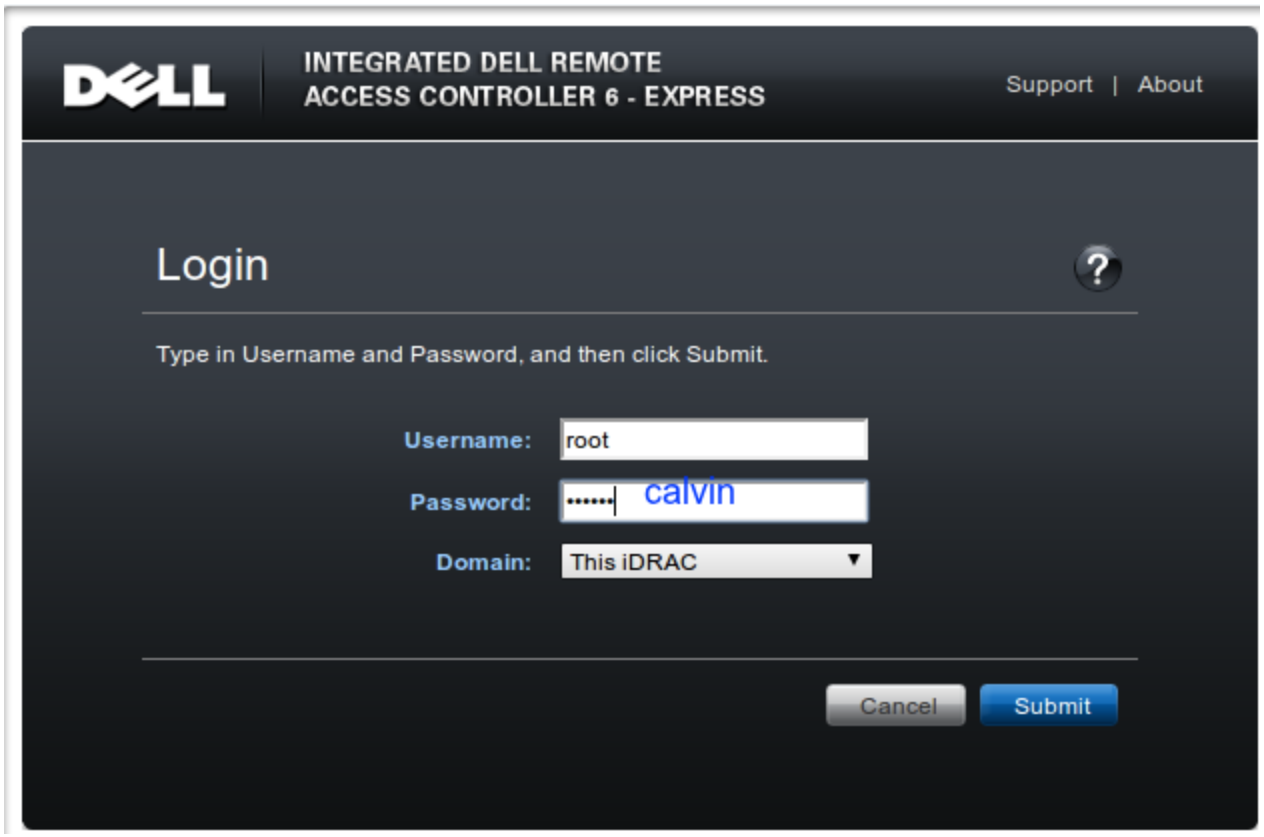
1. Set the IP address on the laptop or PC to **192.168.0.122** with a Subnet mask of **255.255.255.0**.
2. **NOTE:** If your laptop or PC has a Broadcom NIC, you might need to manually set the speed to **100 Full Duplex**.
3. Connect the network cable from the laptop to embedded NIC-1 on the Appliance.

Login to iDRAC Web Interface

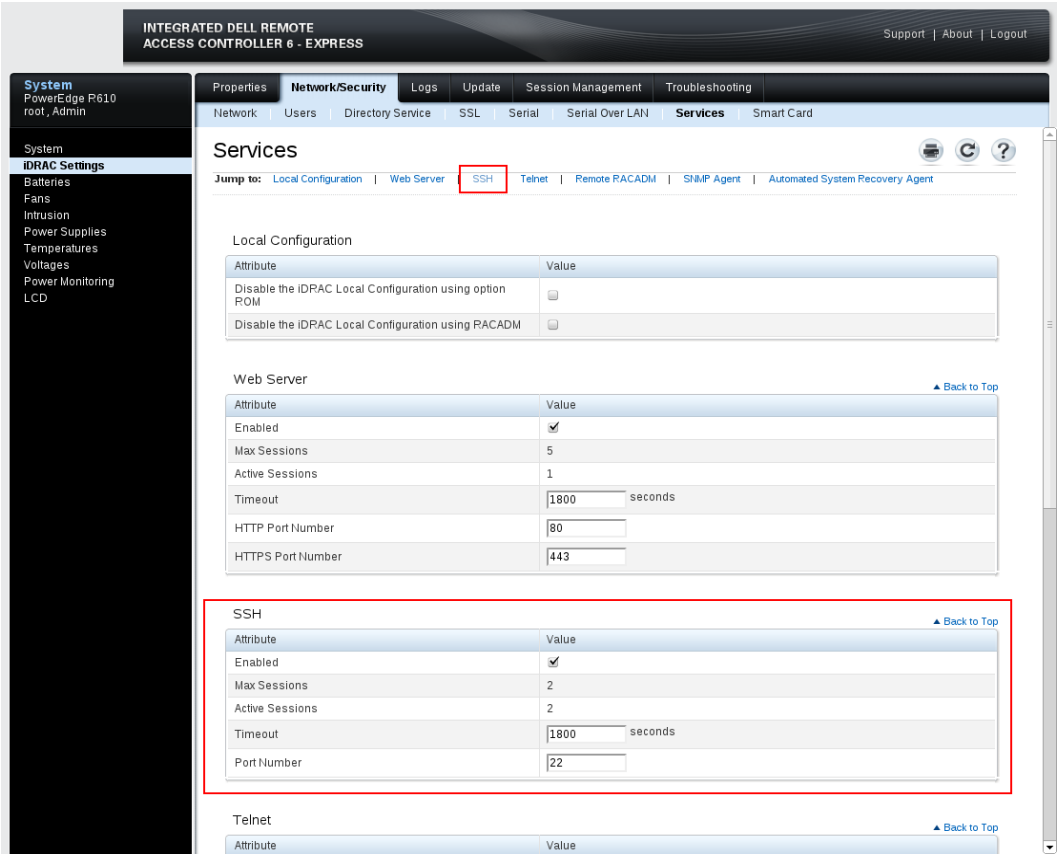
https://192.168.0.120	Default IP address of the iDRAC

To change this you need to go into the BIOS and change the iDRAC network settings options.

User: **root**
Password: **calvin**



Configure SSH access to iDRAC



Login to iDRAC via SSH

```
root@srv1# ssh 192.168.0.120
The authenticity of host '192.168.0.120 (192.168.0.120)' can't be established.
RSA key fingerprint is c5:76:77:e8:8f:86:be:3c:bf:f7:47:7b:c6:e3:10:16.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.120' (RSA) to the list of known hosts.
root@192.168.0.120's password:
/admin1-> help
[Usage]
   show    [<options>] [<target>] [<properties>]
           [<propertyname>== <propertyvalue>]
   set     [<options>] [<target>] <propertyname>=<value>
   cd      [<options>] [<target>]
   create  [<options>] <target> [<property of new target>=<value>]
           [<property of new target>=<value>]
   delete  [<options>] <target>
   exit    [<options>]
   reset   [<options>] [<target>]
   start   [<options>] [<target>]
   stop    [<options>] [<target>]
   version [<options>]
```

```
   help   [<options>] [<help topics>]
   load -source <URI> [<options>] [<target>]
   dump -destination <URI> [<options>] [<target>]

/admin1->
```

Remote Login to iDRAC with ipmitool

Commands

```
ipmitool -v -v -l lan -H 192.168.0.120 -U root -P calvin shell
```

Power On/Off

```
ipmitool> power
chassis power Commands: status, on, off, cycle, reset, diag, soft
ipmitool>
```

Usage

```
ipmitool> help
Commands:
      raw           Send a RAW IPMI request and print response
      i2c           Send an I2C Master Write-Read command and print response
      spd           Print SPD info from remote I2C device
      lan           Configure LAN Channels
      chassis       Get chassis status and set power state
      power         Shortcut to chassis power commands
      event         Send pre-defined events to MC
      mc            Management Controller status and global enables
      sdr           Print Sensor Data Repository entries and readings
      sensor        Print detailed sensor information
      fru           Print built-in FRU and scan SDR for FRU locators
      gendev        Read/Write Device associated with Generic Device locators
sdr
      sel           Print System Event Log (SEL)
      pef           Configure Platform Event Filtering (PEF)
      sol           Configure and connect IPMIv2.0 Serial-over-LAN
      tsol          Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
      isol          Configure IPMIv1.5 Serial-over-LAN
      user          Configure Management Controller users
      channel       Configure Management Controller channels
      session       Print session information
      sunoem        OEM Commands for Sun servers
      kontronoem    OEM Commands for Kontron devices
      picmg         Run a PICMG/ATCA extended cmd
      fwum          Update IPMC using Kontron OEM Firmware Update Manager
      firewall      Configure Firmware Firewall
      shell         Launch interactive IPMI shell
      exec          Run list of commands from file
      set           Set runtime variable for shell and exec
```

```
      hpm           Update HPM components using PICMG HPM.1 file
      ekanalyzer    run FRU-Ekeying analyzer using FRU files

ipmitool>
```

Reference

For further reference please consult the

- iDRAC Manual
- iDRAC Wiki

iDRAC Manual	http://support.dell.com/support/edocs/software/smdrac3/idrac/idrac17mono/en/index.htm
iDRAC Wiki	http://en.wikipedia.org/wiki/Dell_DRAC

Cavium Nitrox

This card provides SSL offloading for the Gateway. What this means is that as the host CPU on the Appliance works on given problems, the SSL portion of the load can be carried out on the SSL offloading card.
It does not require any specific additional set up. You can ensure that it has been loaded by the Gateway process by checking the output of the Gateway trace files.
Near the top of the file you should see the following line:

```
INFO    20/Feb/2012:12:05:42.503 [c30176f0] SSL engine cavium initialized
INFO    20/Feb/2012:12:05:42.508 [c30176f0] engine cavium is default for 'DSA,RSA,DH'
```

Thales nShield Solo Integration

This document describes how to use the Gateway with private keys stored on the Thales (formerly *nCipher*) nShield Solo HSM. You will be shown how to generate and use private keys stored in the HSM's security world.

The Gateway appliance is available with a Thales nShield Solo HSM onboard, if you have one of these appliances then to use private keys you must the following tasks:

- Create a Security World for the HSM
- Generate a new private key or import an existing private key onto the HSM
- Configure the Gateway to use the private key on the HSM

Note this document refers to the "nShield User Guide", this can be found in either of the following locations:

- `/opt/add-ons/ncss-linux64-use/document/nShield_User_Guide.pdf`
- found on the CD "`nCSS-linux64-use`" shipped with HSM appliance, /`nCSS-linux64-use/document/nShield_User_Guide.pdf`

Setting up the HSM

This section explains how to:

- Create a security world for the HSM
- Generate a private key on to the HSM or Import an existing private key on to the Gateway.

Create a Security World for the HSM

You must create a security world so the HSM can be used with the Gateway and other applications for cryptographic operations (see *Creating a Security World* in the *nCipher nShield Solo User Guide)*.

Important: The module must be in pre-initialization mode (see *Appendix I: Checking and Changing Module Mode* in the user guide).

Perform the following steps:

- Set the module to pre-initialization mode (see *Putting a Module in Pre-maintenance Mode* in the user guide).
- Create the security world:
  `# new-world -i -Q 1/2`
  Follow the on-screen instructions (you should have two blank cards to complete it).
  Note: It is recommended that you do not create ACSs for which K is equal to N, because you cannot replace such an ACS if even 1 card is lost or damaged. See *Creating a Security World using new-world* in the user guide for mode details and options.
- Check the status (`mode = initialization`):

```
# enquiry
...
Module #1:
      enquiry reply flags  none
      enquiry reply level  Six
      serial number        XXXX-XXXX-XXXX
      mode                 initialization
      version              X.XX.X
      ...
```

- Check the module world (the output in bold must be non-zero):

```
# nfkminfo -w
World
generation  2
state       0x17270000 Initialised Usable Recovery !PINRecovery !
ExistingClient RTC NVRAM FTO SEEDebug
n_modules   1
hknso       c8b7e7b38455641bf9d0e45a4c9df9d3cc024430
hkm         9df31cb768830d9f0ad4b59fcae57bbc3ea6b4d2 (type DES3)
hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
hkre        cd5d10babb8d6ecaa993b7d61eda9c4cd06af041
hkra        b43682b54fc72abb649b40457506dbeeda5714b5
hkmc        31f541ef92b28f47b134e00fb2a77ab6975911be
hkrtc       7a37e963400821179f470fe39c454a9b0c9bc6b7
hknv        8fff67e0e51e2929cb5533c839aaa862bd619fc9
hkdsee      9cfd7bfc3e545df8b955fc25fc52e76d0fe52848
hkfto       76f4a6cf7c0108ca3dbfa2415e273c71b3235c7f
hkmnull     1d572201be533ebc89f30fdd8f3fac6ca3395bf0
```

```
ex.client   none
k-out-of-n  1/1
other quora m=1 r=1 nv=1 rtc=1 dsee=1 fto=1
createtime  XXXX-XX-XX XX:XX:XX
nso timeout 10 min
```

- Set the module in operational mode (see *Putting a Module in Operational Mode* in the user guide).
- Check the status (`mode=operational`):

```
# enquiry
Module #1:
enquiry reply flags  none
enquiry reply level  Six
serial number        XXXX-XXXX-XXXX
mode                 operational
version              X.XX.X
...
```

When a security world has been created, you can create and manage OCSs and softcards, as well as create, import and manage the keys it protects (see *Chapter 6: Managing Card Sets and Softcards* in the user guide).

Generate a new Private Key on to the HSM

nCipher nShield supports the RSA key type for the Gateway's OpenSSL CHIL engine for all cryptographic operations. The following command shows how to generate a key of `embed` type on the HSM:

```
# generatekey -g embed plainname=key1 type=rsa size=2048
embedsavefile=key1.pem protect=module
```

This will generate an RSA key with name `key1` and size `2048`. The key is added to the HSM key storage (`/opt/nfast/kmdata/local/`). The `key1.pem` file is generated, containing a specially encoded reference to the generated key. A certificate request and a self-signed certificate are also written to the `key1_req.pem` and `key1_selfcert.pem` files respectively.

When you have the certificate and private key, you can import them into the Gateway's certificate store to use for the CHIL engine cryptographic operations in the Gateway.

Note: You may also wish to use the pre-installed KeySafe Java application to manage OCSs, softcards, and keys using its GUI. You must configure it depending on your security environment (see *Appendix A: Using KeySafe* in the user guide).

Importing an existing Private Key on to the HSM

If you already have a set of software keys you can import them into HSM and use the private keys stored on HSM instead for all supported cryptographic operations on the Gateway.

The following key types can be imported to the HSM (for more details see *Chapter 9: Working with keys: Importing keys* in the user guide):

- RSA keys in PEM-encoded PKCS #1 format (with no pass phrase);
- DES, DES2 and Triple DES keys.

The following steps show how to import an RSA key to the HSM as `embed` type from a PKCS12 file:

- Extract RSA private key from PKCS12 file

```
# openssl pkcs12 -in PKCS12.PFX -nocerts -out pkey_encrypted.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

  Note: Make sure the PEM pass phrase contains at least 4 chars.

- Remove the pass phrase from the private key file:

```
# openssl rsa -in pkey_encrypted.pem -out pkey_no_pass.pem
Enter pass phrase for pkey_encrypted.pem:
writing RSA key
```

- Import the private key to HSM:

```
# generatekey --import embed pemreadfile=pkey_no_pass.pem
plainname=importedkey ident=RSAkey1 protect=module
embedsavefile: Filename to write key to? []
> key1.pem
nvram: Blob in NVRAM (needs ACS)? (yes/no) [no] >
key generation parameters:
operation      Operation to perform         import
application    Application                  embed
verify         Verify security of key       yes
type           Key type                     RSA
pemreadfile    PEM file containing RSA key  pkey_no_pass.pem
embedsavefile  Filename to write key to     key1.pem
ident          unknown parameter            RSAkey1
plainname      Key name                     importedkey
nvram          Blob in NVRAM (needs ACS)    no
Key successfully imported.
Path to key: /opt/nfast/kmdata/local/key_embed_xxxxxxxxxxxxxxx
```

Now you have the key1.pem RSA private 'enveloped' key stored on HSM that you may import into the Gateway's certificate store. The key1.pem is not a real private key, but an 'enveloped' key that references the real key protected by HSM. The key1.pem cannot be used for cryptographic operations in isolation, e.g. when the HSM that protects the real key is not accessible, or the real key is removed from the HSM.

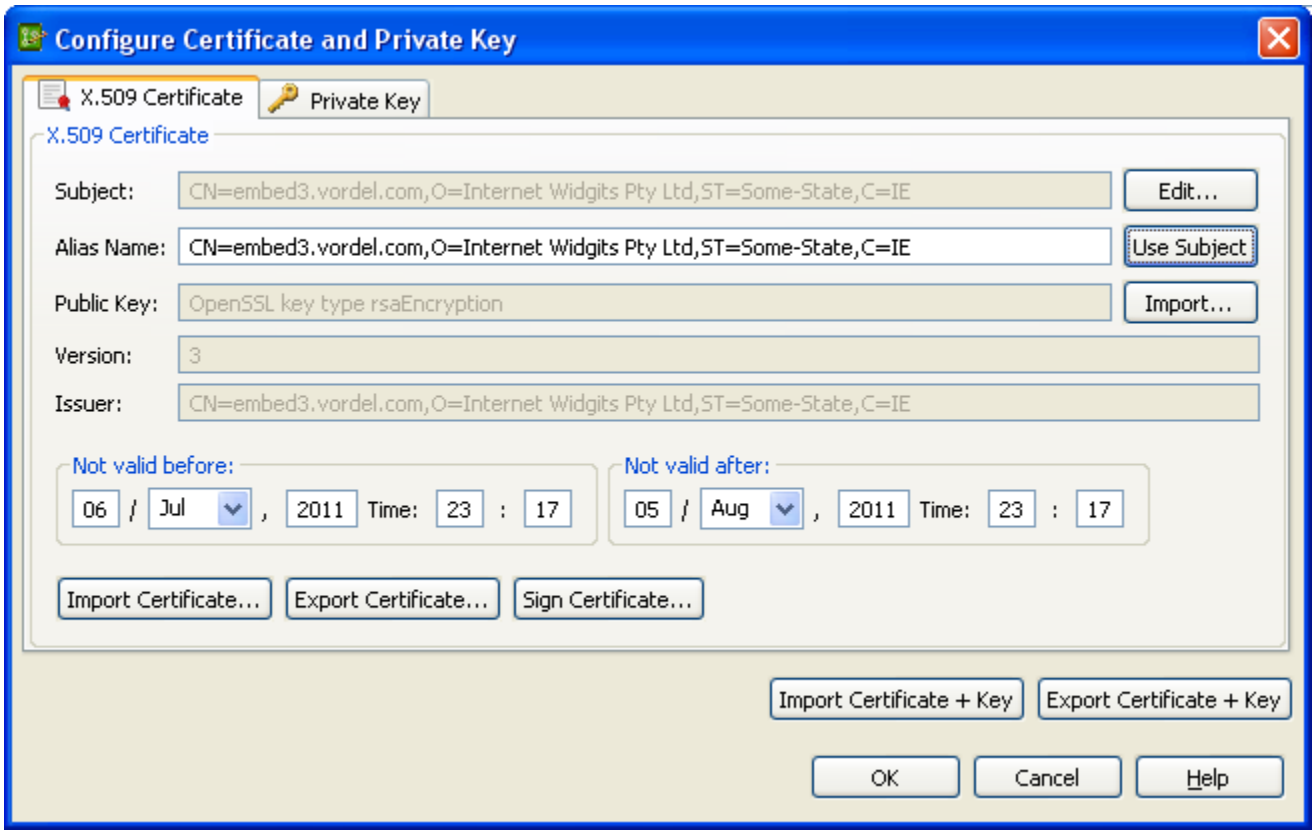
Setting up the Gateway

Importing the Private Key into the Gateway

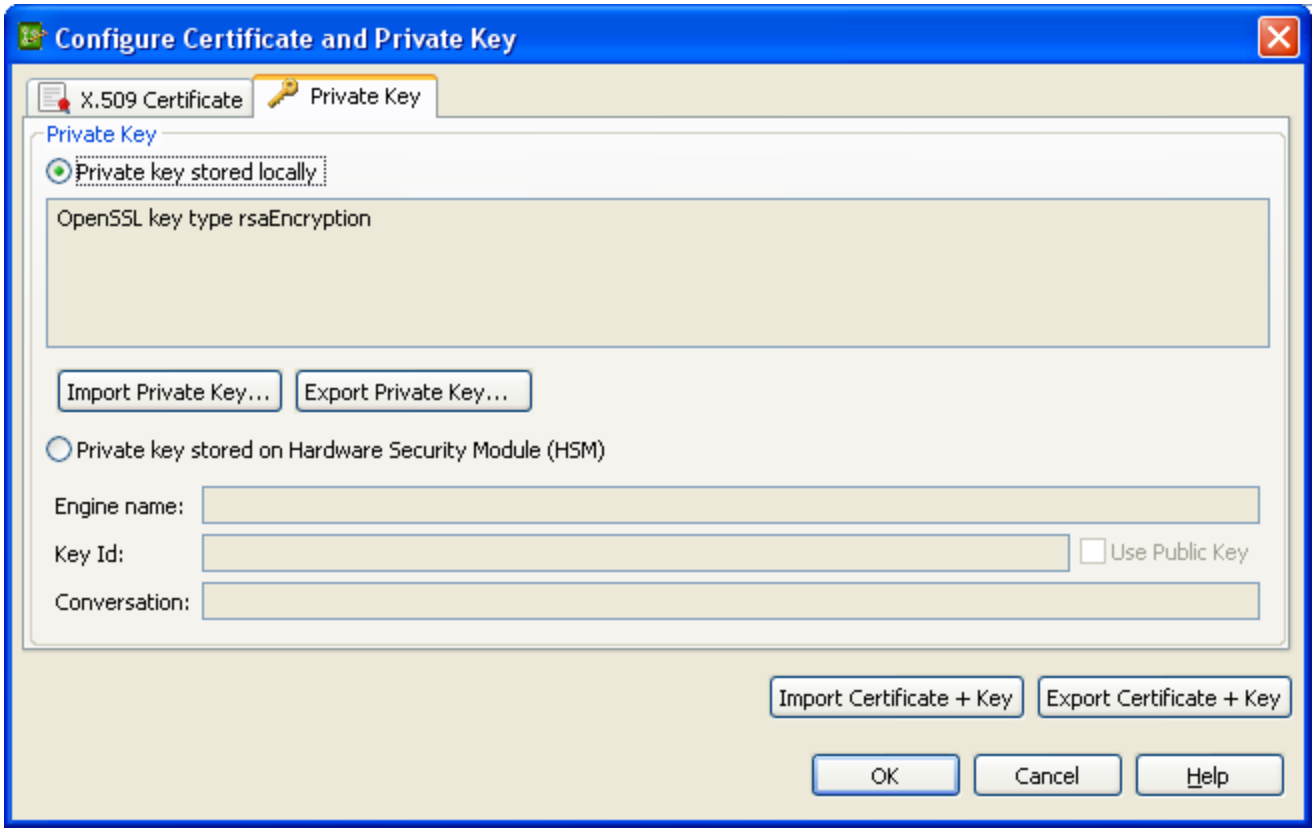
You can import the certificate and private key stored in the HSM using Policy Studio (see Certificate Store in the Gateway Configuration Guide). For example, you have the HSM private 'enveloped' key key1.pem and the self-signed certificate key1_selfcert.pem (see Generating a Private Key on the HSM or Importing a private key to the HSM), open the Configure Certificate and Private Key dialog to import the certificate and the key:

- Click **Import Certificate** in the **X.509 Certificate** pane, and select the `key1_selfcert.pem` file.

Set the **Subject** field as required for the certificate.



- Click the **Private Key** tab. Select the **Private key stored locally** option to import the key.
- Click **Import Private Key...,** and select the `key1.pem` file.
- Click **OK** in the **Enter password** dialog leaving the password field blank (`key1.pem` is not password protected).



Note, the option “Private key stored on Hardware Security Module (HSM)” does **not** need to be selected for Thales nShield Solo HSM, this is required for HSMs from other vendors.

- Click **OK** to save the imported certificate and private key in the Certificate Store.

  Now the Certificate Store contains the certificate with the private ‘enveloped’ key stored and protected in the security world of the nCipher nShield Solo HSM (`/opt/nfast/kmdata/local/`).

You can use this certificate in filters that perform cryptographic operations with the OpenSSL CHIL engine.

Note: If you have set up the HSM with the Gateway software, i.e. you do not have an appliance with HSM then you must tell the Gateway to use the OpenSSL CHIL engine, see Configuring OpenSSL CHIL engine for the Gateway.

Testing the HSM Installation

You may want to check that the HSM is installed successfully and in operational mode:

```
# export PATH=$PATH:/opt/nfast/bin/
# enquiry
```

You should see the following output indicating that the HSM is ready and in operational mode:

```
Server:
      enquiry reply flags  none
```

```
      enquiry reply level  Six
      serial number        XXXX-XXXX-XXXX
      mode                 operational
      version              X.XX.XX
      ...
      product name         nFast server
      ...
Module #1:
      enquiry reply flags  none
      enquiry reply level  Six
      serial number        XXXX-XXXX-XXXX
      mode                 operational
      version              X.XX.X
      ...
      product name         nC1003P/nC3023P/nC3033P
      device name          #1 nFast PCI device, bus X, slot X.
      ...
```

Utimaco CryptoServer

Testing Drivers are Loaded

The file */dev/cs2* should be created automatically when the cs2.ko kernel module is loaded. Check that the cs2 module is loaded using lsmod. The output of dmesg should also display some lines regarding the CryptoServer.

```
# lsmod | grep cs2
cs2                    38980  0
# ls -l /dev/cs2a
crw-r--r-- 1 root root 244, 0 Jun 24 11:37 /dev/cs2a
#  dmesg | grep CryptoServer
[233475.957445] CryptoServer Linux Driver 3.0.4 (DEBUG backlog)
[233475.959960] CryptoServer 0000:04:00.0: PCI INT A -> GSI 38 (level, low) ->
IRQ 38
[233475.961645] CryptoServer 0000:04:00.0: setting latency timer to 64
#
```

Initialising the card

To get the card from initialized to operational mode it is necessary to load the firmware package into the CryptoServer. Utimaco provides csadm, a command line tool which provides all administrative functions needed to setup the CryptoServer.

Add the csadm directory to your path as follows:

```
# PATH=/opt/utimaco/Software/Administration/csadm/Linux_x86_32:$PATH
```

To get the CryptoServer into the operational state run the following command:

```
# csadm Dev=/dev/cs2a
AuthRSAsign=ADMIN,/opt/utimaco/Software/Administration/CAT/key/init_dev_prv.ke
y LoadPKG=/opt/utimaco/Firmware/SecurityServer-2.10.2.mpkg
I: Reading package...
```

```
I: Perform authentication and create session
I: Retrieving file list from CryptoServer
Package /opt/utimaco/Firmware/SecurityServer-2.10.2.mpkg successfully loaded
#
```

Now create a file "/etc/cs_openssl.ini" (obviously replacing the listed users and passwords)

```
[Default]
Device=/dev/cs2a
ConnectTimeout=5000
TCPTimeout=60000
Logging=7
Logpath=/tmp
AuthUser=SHA1Pwd=Axway,fred
```

Add the "Axway" user:

```
# csadm dev=/dev/cs2a
AuthRSAsign=ADMIN,/opt/utimaco/Software/Administration/CAT/key/init_dev_prv.ke
y addusersha1pwd=Axway,00000002,no_login+sm,ask
Enter New Passphrase:
Repeat New Passphrase:
```

(The username and passphrase above must match those in the /etc/cs_openssl.ini file, i.e. Axway and fred).

```
# cp /opt/utimaco/Software/OpenSSL/Linux-i686/ossl_dyn/libcs.so
/opt/gateway/platform/lib/engines/
# cp /opt/utimaco/Software/OpenSSL/Linux-i686/engine-vordel/libcs_oenga.so
/opt/gateway/platform/lib/engines/

# vrun openssl engine -pre
SO_PATH:/opt/utimaco/Software/OpenSSL/Linux-i686/engine-vordel/ cs
max open files:  1048576
(cs) CryptoServer hardware engine support
[Success]: SO_PATH:/opt/utimaco/Software/OpenSSL/Linux-i686/engine-vordel/
```

You should be able to generate RSA keys now:

```
# vrun openssl genrsa -engine cs
max open files:  1048576
engine "cs" set.
Generating RSA private key, 512 bit long modulus
```

Bonding Network Interfaces

Administrators can bind multiple network interfaces together into a single channel with the bonding kernel module and create a special network interface called a channel bonding interface. Channel bonding enables 2 or more network interfaces to act as one. This will increase bandwidth and provide redundancy.

To create a channel bonding interface create a file in the **/etc/sysconfig/network-scripts/** directory called

ifcfg-bond<*N*> , replacing **<*N*>** with the number for the interface, such as **0**

Here is a sample for an appliance **ifcfg-bond0** which uses DHCP but it could just as easily be setup with a static IP address.

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
BOOTPROTO=dhcp
ONBOOT=yes
USERCTL=no
BONDING_OPTS="mode=0 miimon=100"
```

Note about the bonding options: either **miimon** or **arp_interval** and **arp_ip_target** module parameters must be specified, otherwise bonding will not detect link failures! Mode 0 or balance-rr is the Round-robin policy which gives fault tolerance and load balancing. In this mode sends are received on each node in sequential order, so the load is distributed on NICs.
Example of fault tolerant mode with a passive backup and a named primary interface.

```
BONDING_OPTS="mode=1 miimon=100 primary=ethGb1"
```

Then after the channel bonding interface has been created, the network interfaces to be bound together must be configured by adding the **MASTER=** and **SLAVE=** directives to their configuration files. The configuration files for each of the channel-bonded interfaces can be nearly identical. Also add the correct MAC Address for the interface using the HWADDR setting.

cat /etc/sysconfig/network-scripts/ifcfg-ethGb1

```
# Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet
DEVICE=ethGb1
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no
HWADDR=XX:XX:XX:XX:XX:XX
```

cat /etc/sysconfig/network-scripts/ifcfg-ethGb2

```
# Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet
DEVICE=ethGb2
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no
HWADDR=XX:XX:XX:XX:XX:XX
```

For a channel bonding interface to be valid, the kernel module must be loaded. To ensure that the module is loaded when the channel bonding interface is brought up, add the following line to **/etc/modprobe.conf**:

alias bond<*N*> bonding
Replace **<*N*>** with the number of the interface, such as **0** in this example.

System Backup and Recovery

Keeping up-to-date backups of the key system files can be very useful for recovering a system in the case of a disaster. The Appliance provides some tools which make scheduled system backup and system recovery easier to manage.

There are two key backup tasks relating to:

- WAI settings (users, groups, access control, backup tasks, module configuration)
- System Backup

The WAI settings backup can be used to duplicate WAI module changes for mutiple machines in the same environment. Say, for example, that the user wished to configure a new user with restricted module access, and restrict WAI access to office hours access from a given IP address range. This is possible through User Access Control on the WAI. But if the user had 4 Appliances which required the same configuration then the backup of WAI settings from one machine could be duplicated across to the others.

The system backup utility wraps key system configuration files into a tar and gizip compressed file. The files backed up contain configurations related to the:

- firewall
- clock, timezone and NTP
- network settings
- sysctl parameters
- selinux configuration
- API Gateway configuration and settings

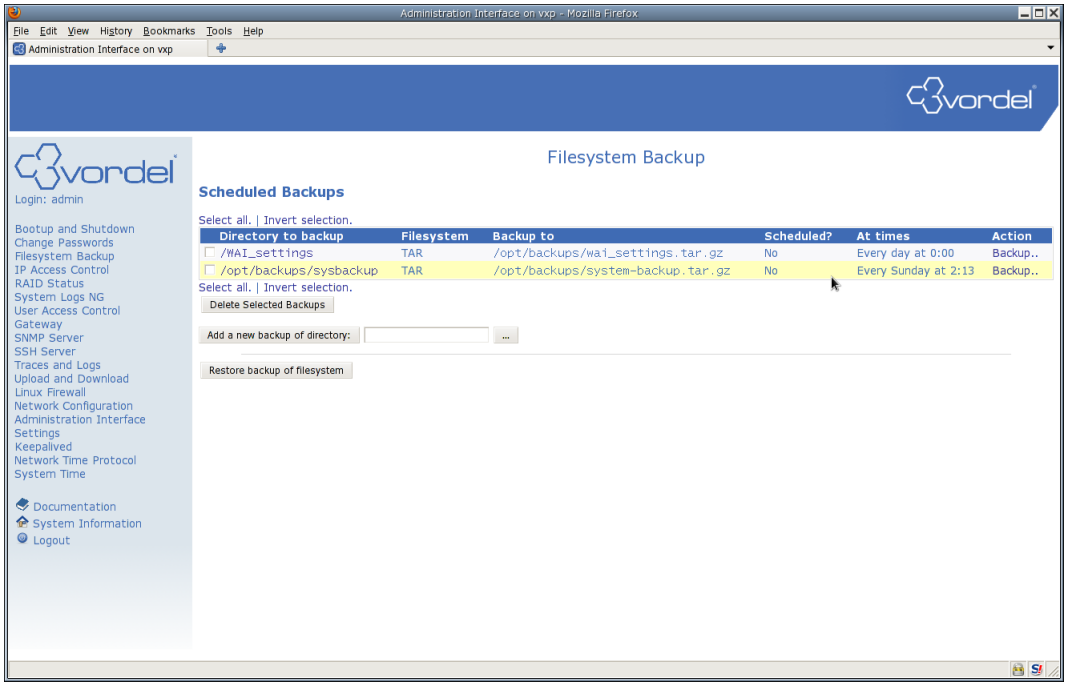
The main use for the system backup task is to aid in server reconfiguration in the case of total failure of a given server requiring reinstallation. This could be due to hardware failure, or some disaster scenario. It is recommended that the system backup is stored remotely.

Setting up System Backup

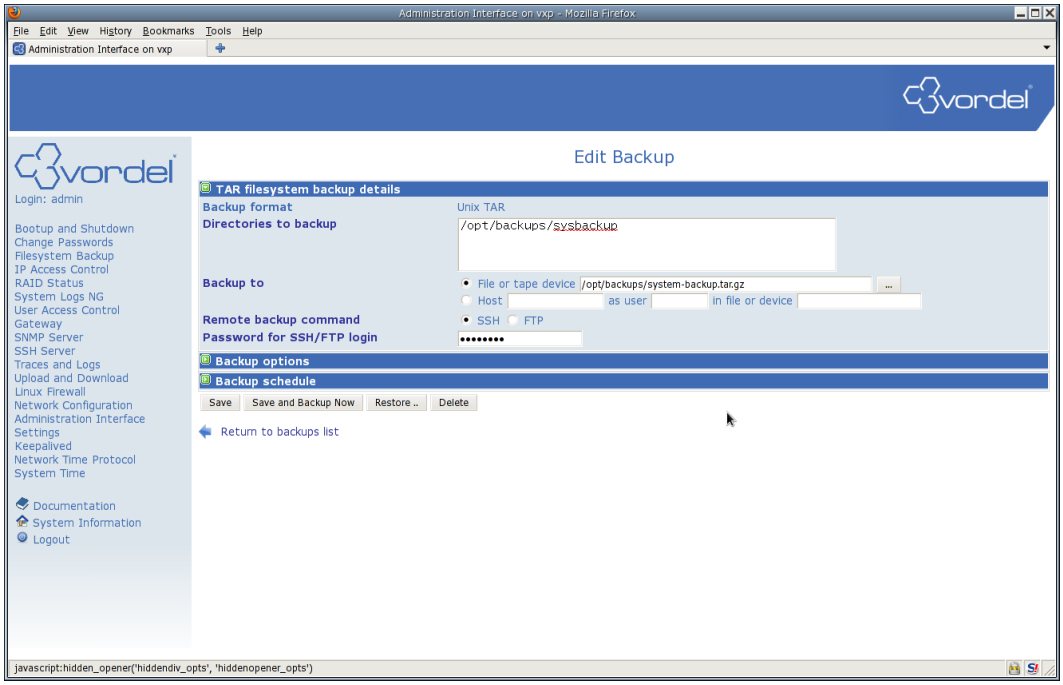
First, install the appliance-system-backup tools, preferably using yum:

```
# yum install -y appliance-system-backup
```

After this you should see the System backup task in Filesystem Backup on the WAI.
By default it is configured to backup the files locally to /opt/backups/system-backup.tar.gz. It is configured (but not scheduled) to run every Sunday night at 2:13 in the morning. It is recommended to change this to a remote backup and either run it after and system adjustments, or schedule it to run automatically at a suitable time for the environment.

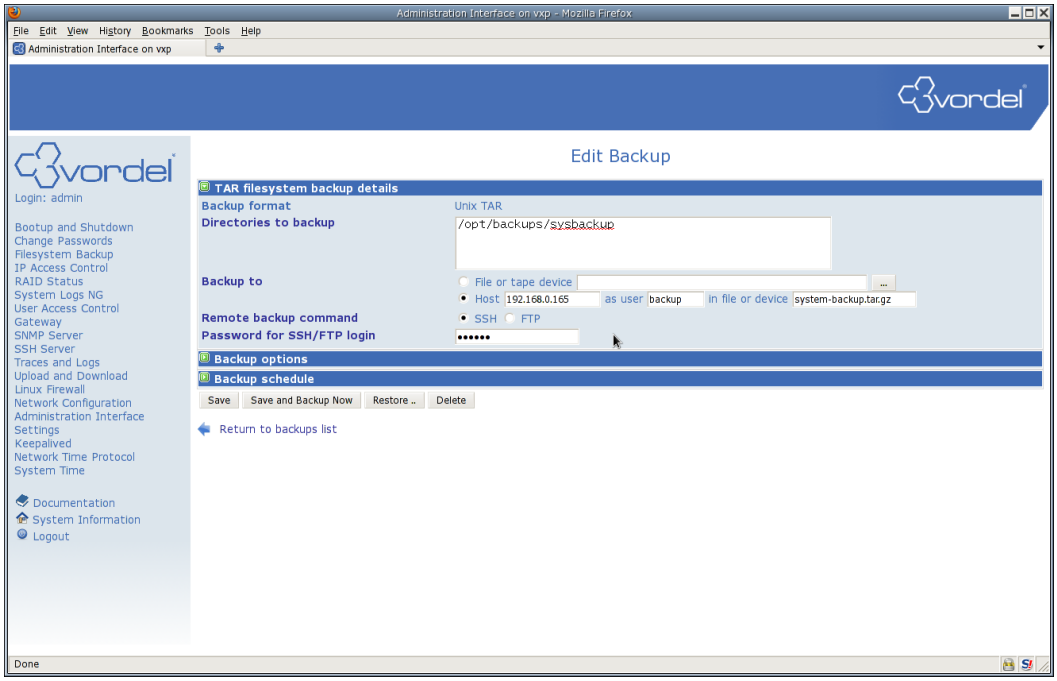


Click on “/opt/backups/sysbackup” to enter the Edit Backup screen

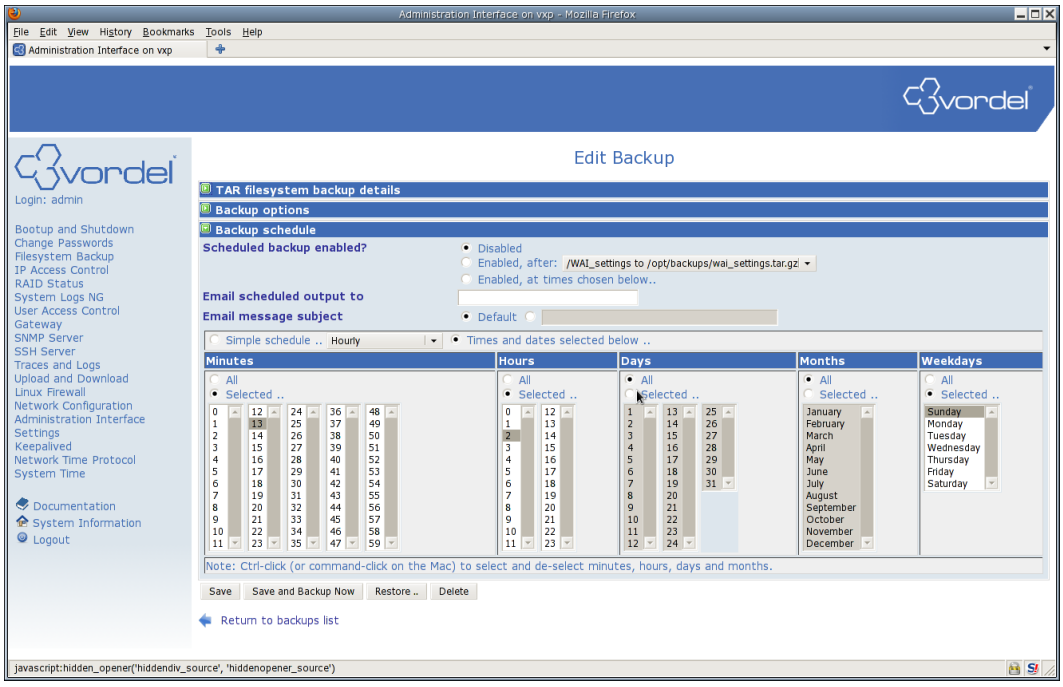


To change this to a remote backup select the option next to Host, then enter the IP address or hostname

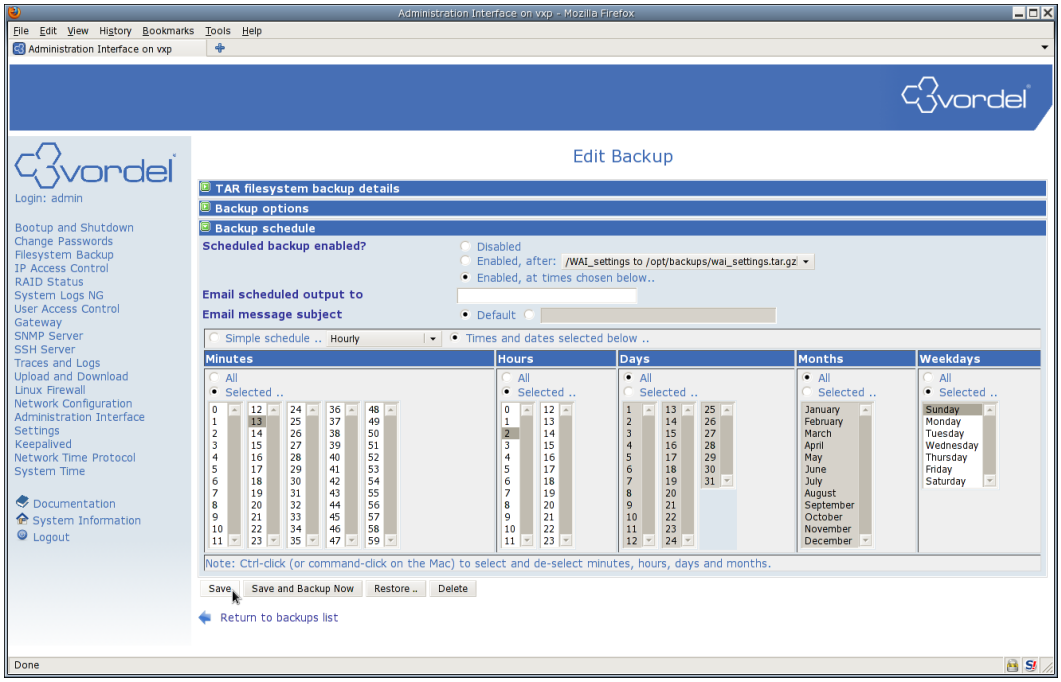
of the host, along with a user, and a filename for the backup. SSH is the recommended remote backup command, and enter the password for the remote user.



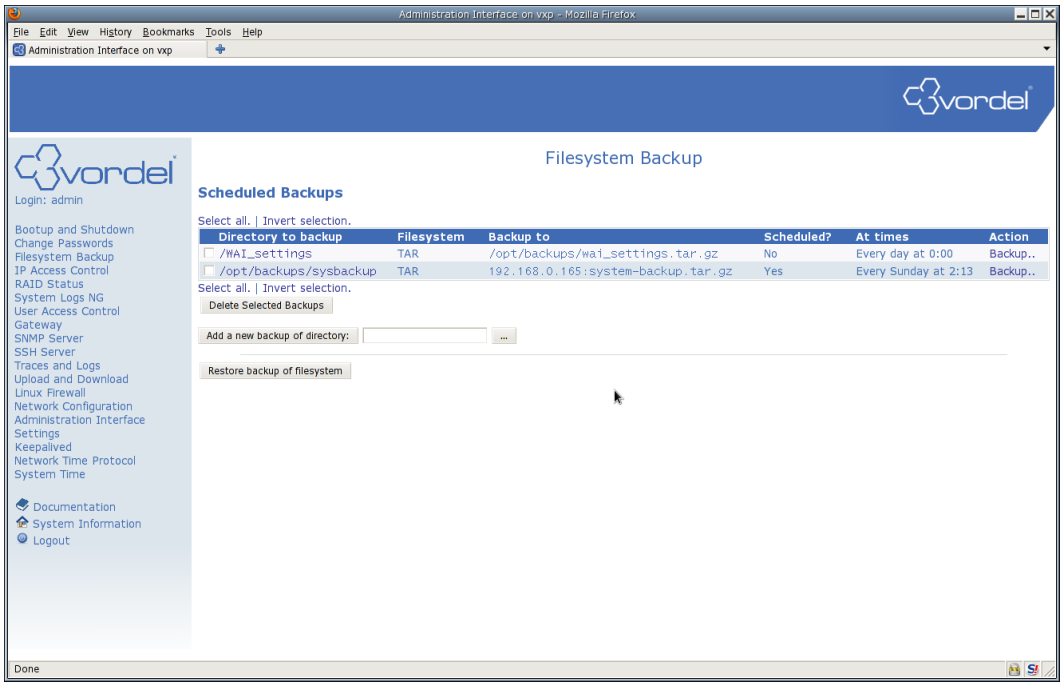
Click the green arrow next to “Backup schedule” if scheduled backup is to be enabled.



Select “Enabled, at times chosen below”. Times can be edited, or just left at 02:13 every Sunday. Click the Save button.



The Filesystem Backup screen should now show the modifications.



An immediate backup can be taken by clicking the “Backup..” link in the Action column.

Restoring a backup file on new system

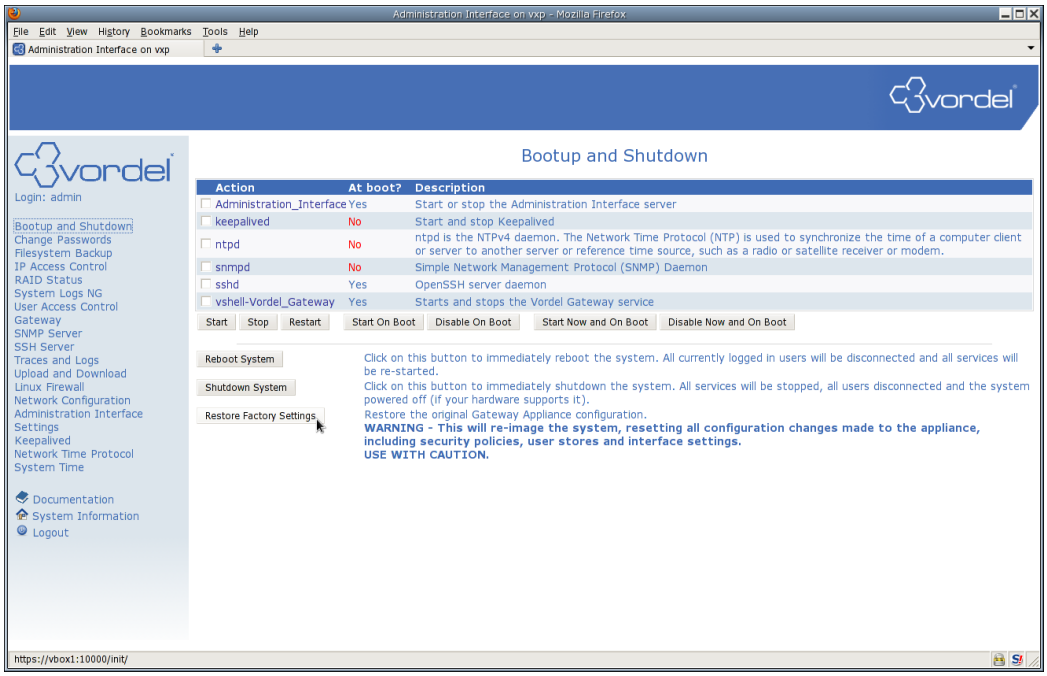
To restore a system backup file on a new system follow these steps:

- Log in as root to the new system
- Stop the API Gateway service if it is running
- Install the appliance-system-backup rpm using yum if it has not already been installed
    - `# yum install -y appliance-system-backup`
- Copy the system backup tar.gz file to the system
- Run the `system-recover.sh` script, giving the name of the backup file as an argument
    - `system-recover.sh system-backup.tar.gz`
- Reboot the system for the changes to take effect. This may change network settings.

Factory Reset

Using the WAI

To factory reset the server log in to the WAI and select Bootup and Shutdown from the Menu. Click on the Restore Factory Settings button.



This will reinstall the system, formatting the hard drive, and completely resetting any changes which have been made since system installation. Caution is advised. It is strongly recommended that the system backup and WAI settings backup has been created before restoring Factory Settings.

After selecting Restore Factory Settings the system will reboot and the re-install will commence.

Grub commands for Unbootable system

If the system is in a state where it will not boot (perhaps due to modification/deletion of key system files) then it can still be possible to factory reset the server from the bootup prompts.

If the factory partition is still intact then it should be possible to call the factory reset manually by following these commands:

At the grub menu press 'c' for the grub command line.
At the `grub>` command prompt enter the following (output shown for clarity):

```
grub> root (hd0,1)
 Filesystem type is ext2fs, partition type 0x83

grub> kernel /vmlinuz ks=hd:sda2:/ks_restore.cfg
   [Linux-bzImage, setup=0x1e00, size=0x1fd65c]

grub> initrd /initrd.img
   [Linux-initrd @ 0z1f7fc000, 0x7e3efc bytes]

grub> boot
```

The system re-install will commence.

Command Line Reference

While the Web Administration Interface is a useful tool it is also possible - and sometimes necessary - to change the system configuration using the command line interface. The base OS for the Appliance is Oracle Enterprise Linux 5.6, and as such, the user has full access to the system using the command line. BASH is the default shell, but KSH and TCSH are also installed and can be used if preferred. For users unfamiliar with the Linux/Unix command line some care must be taken when executing commands (especially as the root user). Executing commands as the root user can have potentially hazardous and irreversible effects on your system. Caution must be exercised if deleting/modifying system files. Having a recent system backup is highly recommended.

Logging in to the Appliance Command Line

After installation is possible to remotely access the Appliance command line using SSH from Linux/Unix/cygwin or PuTTY from a Windows machine. As a security precaution the user cannot directly log in to the *root* account (described earlier in this document). Therefore, the user will have to log in as the *admin* user and switch users to *root* to carry out many of the instructions to follow.

The procedure is as such:

1. Access the system via ssh as *admin*
2. Enter the *admin* password when prompted
3. Enter the command `su -` to switch to the *root* user
4. Enter the *root* password when prompted
5. If the password is entered correctly the prompt should change from `$` to `#`

Example:

```
[admin@appliance ~]$ su -
Password:
[root@appliance ~]
[12:07:40]#
```

Service Commands

The `service` and `chkconfig` commands are used to start/stop and modify runlevels of the */etc/init.d* scripts. This is best explained with some examples. Changes to the runlevels require *root* access.

Starting/Stopping Gateway

After installation of v 6.3.1 of the Appliance the default Gateway service is named *vshell-Vordel_Gateway*.

To start this service execute:

```
# service vshell-Vordel_Gateway start
Starting the Vordel Gateway service                        [  OK  ]
#
```

To stop it:

```
# service vshell-Vordel_Gateway stop
Stopping the Vordel Gateway service                        [  OK  ]
#
```

To restart (stop/start):

```
# service vshell-Vordel_Gateway restart
```

and to get a status of the service:

```
# service vshell-Vordel_Gateway status
Vordel Gateway service is running
#
```

The service command can also be used to get the status of other system services such as the Firewall (iptables).

This will show the status of the firewall and list the active rules if the service is enabled.

```
# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Table: mangle
```

```
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination

Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
6    ACCEPT     112  --  0.0.0.0/0            224.0.0.18
7    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
8    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
9    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
10   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
11   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:8080
12   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:8090
13   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:10000
14   ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:123
15   ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:161
16   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:389
17   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:636
18   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:1521
19   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:3306
20   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with
icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

[root@appliance ~]
[12:17:18]#
```

Enabling/Disabling Services on System Start

The command `chkconfig` can be used to get a list of services and their enabled disabled state on a given runlevel.

```
# chkconfig --list
```

The Appliance operates at runlevel 3.
To find which services are enabled at this runlevel execute:

```
# chkconfig --list | grep "3:on"
```

Conversly, to find which services are disabled at this runlevel execute:

```
# chkconfig --list | grep "3:off"
```

To enable a given service (for example, `sendmail`) at a runlevel execute the following:

```
# chkconfig --level 3 sendmail on
```

Disabling Firewall

To stop and disable the Firewall issue the following commands (output included for clarity):

```
# service iptables stop
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: nat mangle filter         [  OK  ]
Unloading iptables modules:                                [  OK  ]
#

# chkconfig iptables off
```

To ensure that the service is indeed stopped and disabled on subsequent system boots run:

```
# service iptables status
Firewall is stopped.
# chkconfig --list iptables
iptables          0:off 1:off 2:off 3:off 4:off 5:off 6:off
#
```

Updating Software

Software versions and dependencies on the system are managed by RPM and yum.

Yum Commands

To check if there are any new available software updates execute

```
# yum check-update
```

To apply all updates

```
# yum update
```

To apply all updates and automatically answer "yes" to any questions asked by yum

```
# yum update -y
```

To exclude any particular software package form the update use the --exclude option. For example, if the user wished to install all software updates to the OS ***without*** updating the API Gateway version then they would use the command:

```
# yum update -y --exclude=VordelGateway-appliance
```

To search for a specific package run
```
# yum search <keyword>
```

Support can issue important bugfixes or extra functionality for the Appliance through the yum repository. To install a new package such as one of these the user can run
```
# yum install -y <package-name>
```

RPM Commands

It is not recommended that the user run standalone RPM commands to install any package. Yum should be used whenever possible. However, if this cannot be avoided then the rpm command used to install or upgrade a package should be:

```
# rpm -Uvh <package-name>
```

Multiple packages can be specified on the command line. It is sometimes necessary to specify more than one package to the command to satisfy a particular dependency.

Whenever using RPM to install/upgrade a package the output of the above command should be saved.

```
# rpm -qa
```
This command will show all installed package versions. It can be used with `grep` to find specific packages.

```
rpm -qli <package-name>
```
will show all files associated with a package

Installing tar.gz patches

For some specific cases a software patch will be made available through a ‘tarball’ (gzip compressed tar file). To install a file like this on the Appliance the typical method will be either to scp the file to the Appliance or copy it to the system using a USB disk.
To scp the file enter the following command (either from a linux system or using a program like cygwin or WinSCP):

```
# scp gateway-patch-name.tgz admin@appliance-hostname:
```

To copy the file from a USB disk you must:

1. Insert the ext2/3 or FAT32 formatted USB disk in the server
2. Mount the USB. If no modifications to the hard disk layout have been made then the USB should be assigned /dev/sdb. The command to issue in this case would be:
   `mount /dev/sdb1 /mnt/`
3. Copy the file from the USB to the disk
   `cp /mnt/gateway-patch-name.tzg /root/`
4. Umount and remove the USB disk
   `umount /dev/sdb1`

To extract/install the patch, change directory to the location of the tgz file then execute:

```
# tar zxvf gateway-patch-name.tar.gz -C /opt/API/APIgateway
```

as root.

After extracting the files run the following to set the correct ownership on the new files.

```
# chown -R admin:admin /op/API/APIgateway
```

Monitor Server CPU and Memory Usage

System tools such as ps, uptime, top, free, vmstat, iostat and sar are installed on the Appliance and can be used to get a picture of the current state of the system. Much more detail can be found in the **man** pages for each command but the following commands show a very brief introduction into their usage.

```
# ps aux
```

This will give an extended view of all processes currently running on the system. Its output shows among other things the % CPU and % memory monitoring of individual processes

```
# free
```

A simple command which shows the current memory installed on the system and the current usage.

```
# uptime
```

The uptime command gives the system uptime, the current logged in users and the 1, 5, and 15 minute system load average. The load average can give an idea of just how much CPU load the system is under over a each given period of time. It can be useful to determine if the system is experiencing spikes in usage, or sustained heavy CPU usage. The “ideal” load average would be 1 for each of the CPUs on the system. This would indicate that the CPU is being used perfectly over a given time period. Values higher that this indicate that the CPU is busy, and value lower than that indicate that the CPU is idle.

```
# top
```

This is a very useful command which gives a realtime updated summary of the above commands. By default it stacks the processes by CPU usage, but by entering ‘M’ it will cause the list to be sorted by % memory usage.

```
# vmstat
```

This command will report on processes, the memory usage, swap memory, some brief io stats and the state of the cpu. Adding a ‘1’ to the command as an argument will cause it to update every second e.g.

```
# vmstat 1
```

```
# iostat
```

This breaks down the activity to the input/output devices based on average read/write time and by partition. It makes it easier to see where i/o time is being spent.

```
# sar
```

The sar tool can be used to collect and view system information. A typical use for it would be to monitor system usage over a long period of time. The details for setting up this command are beyond the scope of this document and are much better described by reading the **man** page for sar. This can be accessed from the command line by running `# man sar`

View Network Settings

To view the current IP address information use the command `ifconfig`. This will output the newtork information for the currently enabled interfaces.

```
# ifconfig
ethGb1    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:C7
          inet addr:192.168.0.165  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2002:a00:701:0:16fe:b5ff:fed8:9bc7/64 Scope:Global
          inet6 addr: fe80::16fe:b5ff:fed8:9bc7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:624808047 errors:0 dropped:0 overruns:0 frame:0
          TX packets:591961015 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:575050398793 (535.5 GiB)  TX bytes:579919838748 (540.0 GiB)
          Interrupt:36 Memory:d2000000-d2012800

ethGb2    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:C9
          inet addr:192.168.200.200  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 2002:a00:701:0:16fe:b5ff:fed8:9bc9/64 Scope:Global
          inet6 addr: fe80::16fe:b5ff:fed8:9bc9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6373411 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5507122252 (5.1 GiB)  TX bytes:2858 (2.7 KiB)
          Interrupt:48 Memory:d4000000-d4012800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:175076 errors:0 dropped:0 overruns:0 frame:0
          TX packets:175076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:95412457 (90.9 MiB)  TX bytes:95412457 (90.9 MiB)
```

Passing the `-a` switch to the command will give all interaces on the system (whether they are configured or not).

```
# ifconfig -a
ethGb1    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:C7
          inet addr:192.168.0.165  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2002:a00:701:0:16fe:b5ff:fed8:9bc7/64 Scope:Global
          inet6 addr: fe80::16fe:b5ff:fed8:9bc7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:624808092 errors:0 dropped:0 overruns:0 frame:0
          TX packets:591961027 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:575050403673 (535.5 GiB)  TX bytes:579919841844 (540.0 GiB)
```

```
          Interrupt:36 Memory:d2000000-d2012800

ethGb2    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:C9
          inet addr:192.168.200.200  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 2002:a00:701:0:16fe:b5ff:fed8:9bc9/64 Scope:Global
          inet6 addr: fe80::16fe:b5ff:fed8:9bc9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6373439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5507125544 (5.1 GiB)  TX bytes:2858 (2.7 KiB)
          Interrupt:48 Memory:d4000000-d4012800

ethGb3    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:CB
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:32 Memory:d6000000-d6012800

ethGb4    Link encap:Ethernet  HWaddr 14:FE:B5:D8:9B:CD
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:42 Memory:d8000000-d8012800

ethGb5    Link encap:Ethernet  HWaddr 00:10:18:BA:F1:08
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:38 Memory:da000000-da012800

ethGb6    Link encap:Ethernet  HWaddr 00:10:18:BA:F1:0A
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:45 Memory:dc000000-dc012800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
          RX packets:175076 errors:0 dropped:0 overruns:0 frame:0
          TX packets:175076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:95412457 (90.9 MiB)  TX bytes:95412457 (90.9 MiB)
```

To see any routing information use `ip route show`

```
# ip route show
192.168.0.0/24 dev ethGb1  proto kernel  scope link  src 192.168.0.165
169.254.0.0/16 dev ethGb2  scope link
192.168.0.0/16 dev ethGb2  proto kernel  scope link  src 192.168.200.200
default via 192.168.0.3 dev ethGb1
```

When using keepalived for failover you can use `ip addr show` to see if a particular interface is serving the Virtual IP address.

```
# ip addr show
1: lo: mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ethGb1: mtu 1500 qdisc mq qlen 1000
    link/ether 14:fe:b5:d8:9b:c7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.165/24 brd 192.168.0.255 scope global ethGb1
    inet 192.168.0.221/24 brd 192.168.0.255 scope global ethGb1 extra virtual
    inet6 2002:a00:701:0:16fe:b5ff:fed8:9bc7/64 scope global dynamic
       valid_lft 2591881sec preferred_lft 604681sec
    inet6 fe80::16fe:b5ff:fed8:9bc7/64 scope link
       valid_lft forever preferred_lft forever
3: ethGb2: mtu 1500 qdisc mq qlen 1000
    link/ether 14:fe:b5:d8:9b:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.200/16 brd 192.168.255.255 scope global ethGb2
    inet6 2002:a00:701:0:16fe:b5ff:fed8:9bc9/64 scope global dynamic
       valid_lft 2591881sec preferred_lft 604681sec
    inet6 fe80::16fe:b5ff:fed8:9bc9/64 scope link
       valid_lft forever preferred_lft forever
4: ethGb3: mtu 1500 qdisc noop qlen 1000
    link/ether 14:fe:b5:d8:9b:cb brd ff:ff:ff:ff:ff:ff
5: ethGb4: mtu 1500 qdisc noop qlen 1000
    link/ether 14:fe:b5:d8:9b:cd brd ff:ff:ff:ff:ff:ff
6: ethGb5: mtu 1500 qdisc noop qlen 1000
    link/ether 00:10:18:ba:f1:08 brd ff:ff:ff:ff:ff:ff
7: ethGb6: mtu 1500 qdisc noop qlen 1000
    link/ether 00:10:18:ba:f1:0a brd ff:ff:ff:ff:ff:ff
#
```

NIC statistics for a particular interface can be seen by using `ethtool`. This can be useful to detect any

errors or dropped packets at the network level.

```
# ethtool -S ethGb1
NIC statistics:
     rx_bytes: 575050777107
     rx_error_bytes: 0
     tx_bytes: 579919858796
     tx_error_bytes: 0
     rx_ucast_packets: 623336409
     rx_mcast_packets: 104953
     rx_bcast_packets: 1370388
     tx_ucast_packets: 591960894
     tx_mcast_packets: 5
     tx_bcast_packets: 223
     tx_mac_errors: 0
     tx_carrier_errors: 0
     rx_crc_errors: 0
     rx_align_errors: 0
     tx_single_collisions: 0
     tx_multi_collisions: 0
     tx_deferred: 0
     tx_excess_collisions: 0
     tx_late_collisions: 0
     tx_total_collisions: 0
     rx_fragments: 0
     rx_jabbers: 0
     rx_undersize_packets: 0
     rx_oversize_packets: 0
     rx_64_byte_packets: 822932
     rx_65_to_127_byte_packets: 192118010
     rx_128_to_255_byte_packets: 2436169
     rx_256_to_511_byte_packets: 44374203
     rx_512_to_1023_byte_packets: 25331444
     rx_1024_to_1522_byte_packets: 359736870
     rx_1523_to_9022_byte_packets: 0
     tx_64_byte_packets: 3730692
     tx_65_to_127_byte_packets: 105086741
     tx_128_to_255_byte_packets: 3744087
     tx_256_to_511_byte_packets: 95324821
     tx_512_to_1023_byte_packets: 67990101
     tx_1024_to_1522_byte_packets: 316084680
     tx_1523_to_9022_byte_packets: 0
     rx_xon_frames: 3939
     rx_xoff_frames: 3939
     tx_xon_frames: 0
     tx_xoff_frames: 0
     rx_mac_ctrl_frames: 0
     rx_filtered_packets: 551606
     rx_ftq_discards: 0
```

```
     rx_discards: 0
     rx_fw_discards: 0
```

Network Restart

If a network restart is required the `service` command can be used.

```
# service network restart
```

Dell OpenManage Commands

Dell open manage can be used to monitor the state of the system hardware. Usage of the tools is listed here.

Omreport

The `omreport` command reports on a given system subsection. The subsections can be listed with a '?' supplied to the command.

```
# omreport -?

omreport         Reports component properties.

The available command(s) are:

Command          Description
about            Product and version properties.
system           System component properties.
rac              Command not supported. Use the racadm utility.
chassis          Chassis component properties.
storage          Display storage component properties.
```

Chassis Reports

This gives a report of the overall hardware in the server.

```
# omreport chassis
Health

Main System Chassis

SEVERITY : COMPONENT
Ok       : Fans
Ok       : Intrusion
Ok       : Memory
Ok       : Power Supplies
Ok       : Power Management
Ok       : Processors
Ok       : Temperatures
Ok       : Voltages
```

```
Ok       : Hardware Log
Ok       : Batteries
```

omreport chassis bmc

To see iDRAC / IPMI settings specify bmc (Baseboard Management Controller) to the command.

```
appliance:~# omreport chassis bmc
Remote Access Information

Remote Access Device
Attribute : Device Type
Value     : iDRAC6 Express

Attribute : IPMI Version
Value     : 2.0

Attribute : System GUID
Value     : 2020204f-c080-2080-2010-00004c4c4544

Attribute : Number of Possible Active Sessions
Value     : 5

Attribute : Number of Current Active Sessions
Value     : 0

Attribute : Enable IPMI Over LAN
Value     : Yes

Attribute : SOL Enabled
Value     : Yes

Attribute : MAC Address
Value     : 14-FE-B5-D1-57-3B


IPv4 Address
Attribute : IP Address Source
Value     : DHCP

Attribute : IP Address
Value     : 192.168.0.152

Attribute : IP Subnet
Value     : 255.255.255.0

Attribute : IP Gateway
Value     : 192.168.0.3
```

omreport chassis Batteries

```
# omreport chassis Batteries
Batteries

Health : Ok

Individual Battery Elements
Index      : 0
Status     : Ok
Probe Name : System Board CMOS Battery
Reading    : Good
```

omreport storage vdisk

```
# omreport storage vdisk
List of Virtual Disks in the System

Controller PERC 6/i Integrated (Embedded)
ID                  : 0
Status              : Ok
Name                : Virtual Disk 0
State               : Ready
Progress            : Not Applicable
Layout              : RAID-1
Size                : 136.13 GB (146163105792 bytes)
Device Name         : /dev/sda
Bus Protocol        : SAS
Media               : HDD
Read Policy         : No Read Ahead
Write Policy        : Write Back
Cache Policy        : Not Applicable
Stripe Element Size : 64 KB
Disk Cache Policy   : Disabled
```

omreport storage battery

```
# omreport storage battery
List of Batteries in the System

Controller PERC 6/i Integrated (Slot Embedded)
ID                        : 0
Status                    : Ok
Name                      : Battery 0
State                     : Ready
Recharge Count            : Not Applicable
Max Recharge Count        : Not Applicable
Predicted Capacity Status : Ready
Learn State               : Idle
Next Learn Time           : 41 days 6 hours
Maximum Learn Delay       : 7 days 0 hours
Learn Mode                : Auto
```

omreport system summary

This command provides a lot of useful system data including the Service Tag, kernel, memory configuration, network settings etc.

```
# omreport system summary
System Summary

------------------
Software Profile
------------------
Systems Management
Name                       : Information not available.
Version                    : 3.6.0
Description                : Systems Management Software

Operating System
Name                       : Linux
Version                    : Kernel 2.6.32.200(x86_64)
System Time                : Wed Oct 26 17:05:08 2011
System Bootup Time         : Wed Oct 26 16:39:00 2011

--------
System
--------
System
Host Name                  : appliance
System Location            : Please set the value
Life Cycle Controller      : Enabled

---------------------
Main System Chassis
---------------------
Chassis Information
Chassis Model              : PowerEdge R610
System Revision            : II
Chassis Service Tag        :
Chassis Lock               : Present
Chassis Asset Tag          : FZBHY4J

Remote Access Information
Remote Access Device       : iDRAC6 Express

Processor 1
Processor Brand            : Intel(R) Xeon(R) CPU           E5620  @ 2.40GHz
Processor Version          : Model 44 Stepping 2
Voltage                    : 1200 mV

Processor 2
Processor Brand            : Intel(R) Xeon(R) CPU           E5620  @ 2.40GHz
Processor Version          : Model 44 Stepping 2
Voltage                    : 1200 mV

Memory
Total Installed Capacity   : 6144  MB
```

```
Memory Available to the OS : 3276  MB
Total Maximum Capacity     : 196608  MB
Memory Array Count         : 1

Memory Array 1
Location                   : System Board or Motherboard
Use                        : System Memory
Installed Capacity         : 6144  MB
Maximum Capacity           : 196608  MB
Slots Available            : 12
Slots Used                 : 6
ECC Type                   : Multibit ECC

Slot PCI1
Adapter                    : [Not Occupied]
Type                       : PCI E Gen 2
Data Bus Width             : 8x or x8
Speed                      : [Not Obtained, see card documentation]
Slot Length                : Long
Voltage Supply             : 3.3 Volts

Slot PCI2
Adapter                    : Nitrox XL NPX
Type                       : PCI E Gen 2
Data Bus Width             : 8x or x8
Speed                      : [Not Obtained, see card documentation]
Slot Length                : Long
Voltage Supply             : 3.3 Volts

BIOS Information
Manufacturer               : Dell Inc.
Version                    : 3.0.0
Release Date               : 01/31/2011

Firmware Information
Name                       : iDRAC6
Version                    : 1.57

--------------
Network Data
--------------
Network Interface 0
IP Address                 : 192.168.0.158
Subnet Mask                : 255.255.255.0
Default Gateway            : 192.168.0.3
MAC Address                : 14:FE:B5:D1:57:33

Network Interface 1
IP Address                 : [No Value]
MAC Address                : 14:FE:B5:D1:57:35

Network Interface 2
IP Address                 : [No Value]
MAC Address                : 14:FE:B5:D1:57:37
```

```
Network Interface 3
IP Address                    : [No Value]
MAC Address                   : 14:FE:B5:D1:57:39

--------------------
Storage Enclosures
--------------------
Storage Enclosures
Name                          : Backplane
Service Tag                   : 09K3440
```

Upgrade Dell Bios

This section describes the tools available from dell to enable BIOS updates.

For further information see these links
http://linux.dell.com/repo/hardware/latest/
http://linux.dell.com/wiki/index.php/Repository/OMSA

Check Bios Details before run

dmidecode 2.11
SMBIOS 2.5 present.
67 structures occupying 3404 bytes.
..
..
..
Handle 0x0100, DMI type 1, 27 bytes
System Information
    Manufacturer: **Dell Inc.**
    Product Name: **PowerEdge 1950**
    Version: Not Specified
    Serial Number: 172BS3J
    UUID: 44454C4C-3700-1032-8042-B1C04F53334A
    Wake-up Type: Power Switch
    SKU Number: Not Specified
    Family: Not Specified

Installing firmware-tools to manage BIOS and firmware updates

yum install dell_ft_install
yum install $(bootstrap_firmware)

Command 1 *yum install dell_ft_install*

yum install dell_ft_install

```
Loaded plugins: security
dell-omsa-indep                                                 1333/1333
dell-omsa-specific                                        | 1.9 kB     00:00
dell-omsa-specific/primary                                | 164 kB     00:01
dell-omsa-specific                                              1333/1333
el5_addons                                                | 951 B     00:00
el5_addons/primary                                        |  29 kB     00:00
el5_addons                                                      138/138
el5_oracle_addons                                         |  951 B     00:00
el5_oracle_addons/primary                                 | 1.7 kB     00:00
el5_oracle_addons                                               7/7
kingsofsoa                                                |  951 B     00:00
kingsofsoa/primary                                        | 690 kB     00:00
kingsofsoa                                                      971/971
ol5_u6_base                                               | 1.1 kB     00:00
ol5_u6_base/primary                                       | 1.5 MB     00:09
ol5_u6_base                                                     4551/4551
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package dell_ft_install.noarch 0:1.1-1 set to be updated
--> Processing Dependency: dell_ie_idrac7 for package: dell_ft_install
--> Processing Dependency: dell_ie_tape_ibm for package: dell_ft_install
--> Processing Dependency: dell_ie_rac_5 for package: dell_ft_install
--> Processing Dependency: dell_ie_maser_inv_lcl for package: dell_ft_install
--> Processing Dependency: dell_ie_tape_prostor for package: dell_ft_install
--> Processing Dependency: dell_ie_tape_tandberg for package: dell_ft_install
--> Processing Dependency: dell_ie_imc for package: dell_ft_install
--> Processing Dependency: dell_ie_bios for package: dell_ft_install
--> Processing Dependency: dell_ie_tape_quantum for package: dell_ft_install
--> Processing Dependency: dell_ie_bp for package: dell_ft_install
--> Processing Dependency: dell_ie_bmc for package: dell_ft_install
--> Processing Dependency: dell_ie_sas for package: dell_ft_install
--> Processing Dependency: dell_ie_nitrogen for package: dell_ft_install
--> Running transaction check
---> Package dell_ie_bios.x86_64 0:3.1.0-4.143.2.el5 set to be updated
--> Processing Dependency: dell_ft_ie_interface for package: dell_ie_bios
--> Processing Dependency: libsmal.so.0()(64bit) for package: dell_ie_bios
---> Package dell_ie_bmc.i386 0:1.1.0-7 set to be updated
---> Package dell_ie_bp.i386 0:1.1.0-7 set to be updated
---> Package dell_ie_idrac7.x86_64 0:2.0.0-4.10.1.el5 set to be updated
---> Package dell_ie_imc.x86_64 0:1.0.0-4.4.288.el5 set to be updated
--> Processing Dependency: libipmi.so.0()(64bit) for package: dell_ie_imc
---> Package dell_ie_maser_inv_lcl.x86_64 0:3.2.0-4.28.2.el5 set to be updated
--> Processing Dependency: dell_ie_maser for package: dell_ie_maser_inv_lcl
---> Package dell_ie_nitrogen.x86_64 0:2.0.0-4.22.1.el5 set to be updated
---> Package dell_ie_rac_5.x86_64 0:7.0.0-4.1.8.el5 set to be updated
---> Package dell_ie_sas.x86_64 0:3.2.0-4.2.2.el5 set to be updated
---> Package dell_ie_tape_ibm.x86_64 0:1.1.0-7 set to be updated
---> Package dell_ie_tape_prostor.i386 0:1.1.0-7 set to be updated
---> Package dell_ie_tape_quantum.x86_64 0:1.1.0-7 set to be updated
---> Package dell_ie_tape_tandberg.i386 0:1.1.0-7 set to be updated
--> Running transaction check
---> Package dell_ft_ie_interface.noarch 0:1.0.13-4.22.64.el5 set to be updated
--> Processing Dependency: firmware-tools >= 2.0.0 for package: dell_ft_ie_interface
--> Processing Dependency: firmware-addon-dell >= 2.0 for package: dell_ft_ie_interface
---> Package dell_ie_maser.x86_64 0:3.2.0-4.28.2.el5 set to be updated
```

---> Package libipmi0.x86_64 0:1.0.0-4.4.2.el5 set to be updated
---> Package libsmal0.x86_64 0:3.1.0-4.142.1.el5 set to be updated
--> Running transaction check
---> Package firmware-addon-dell.x86_64 0:2.2.2-4.2.393.el5 set to be updated
--> Processing Dependency: python-smbios for package: firmware-addon-dell
--> Processing Dependency: smbios-utils for package: firmware-addon-dell
---> Package firmware-tools.noarch 0:2.1.14-4.14.2.el5 set to be updated
--> Running transaction check
---> Package python-smbios.x86_64 0:2.2.27-3.2.el5 set to be updated
--> Processing Dependency: python-ctypes for package: python-smbios
---> Package smbios-utils.x86_64 0:2.2.27-3.2.el5 set to be updated
--> Processing Dependency: smbios-utils-python for package: smbios-utils
--> Running transaction check
---> Package python-ctypes.x86_64 0:1.0.2-1.2.el5 set to be updated
---> Package smbios-utils-python.x86_64 0:2.2.27-3.2.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

Package	Arch	Version	Repository	Size
Installing:				
dell_ft_install	noarch	1.1-1	dell-omsa-indep	2.7 k
Installing for dependencies:				
dell_ft_ie_interface	noarch	1.0.13-4.22.64.el5	dell-omsa-specific	24 k
dell_ie_bios	x86_64	3.1.0-4.143.2.el5	dell-omsa-specific	51 k
dell_ie_bmc	i386	1.1.0-7	dell-omsa-specific	1.5 M
dell_ie_bp	i386	1.1.0-7	dell-omsa-specific	1.5 M
dell_ie_idrac7	x86_64	2.0.0-4.10.1.el5	dell-omsa-specific	58 k
dell_ie_imc	x86_64	1.0.0-4.4.288.el5	dell-omsa-specific	28 k
dell_ie_maser	x86_64	3.2.0-4.28.2.el5	dell-omsa-specific	115 k
dell_ie_maser_inv_lcl	x86_64	3.2.0-4.28.2.el5	dell-omsa-specific	4.1 k
dell_ie_nitrogen	x86_64	2.0.0-4.22.1.el5	dell-omsa-specific	58 k
dell_ie_rac_5	x86_64	7.0.0-4.1.8.el5	dell-omsa-specific	4.3 k
dell_ie_sas	x86_64	3.2.0-4.2.2.el5	dell-omsa-specific	217 k
dell_ie_tape_ibm	x86_64	1.1.0-7	dell-omsa-specific	482 k
dell_ie_tape_prostor	i386	1.1.0-7	dell-omsa-specific	168 k
dell_ie_tape_quantum	x86_64	1.1.0-7	dell-omsa-specific	120 k
dell_ie_tape_tandberg	i386	1.1.0-7	dell-omsa-specific	21 k
firmware-addon-dell	x86_64	2.2.2-4.2.393.el5	dell-omsa-specific	51 k
firmware-tools	noarch	2.1.14-4.14.2.el5	dell-omsa-specific	221 k
libipmi0	x86_64	1.0.0-4.4.2.el5	dell-omsa-specific	129 k

```
libsmal0                    x86_64          3.1.0-4.142.1.el5          dell-omsa-specific
987 k
python-ctypes               x86_64          1.0.2-1.2.el5              dell-omsa-specific
215 k
python-smbios               x86_64          2.2.27-3.2.el5             dell-omsa-specific
70 k
smbios-utils                x86_64          2.2.27-3.2.el5             dell-omsa-specific
13 k
smbios-utils-python         x86_64          2.2.27-3.2.el5             dell-omsa-specific
63 k

Transaction Summary
================================================================================
================================================================================
Install      24 Package(s)
Upgrade       0 Package(s)

Total download size: 6.1 M
Is this ok [y/N]: y
Downloading Packages:
(1/24): dell_ft_install-1.1-1.noarch.rpm                   | 2.7 kB     00:00
(2/24): dell_ie_maser_inv_lcl-3.2.0-4.28.2.el5.x86_64.rpm  | 4.1 kB
00:00
(3/24): dell_ie_rac_5-7.0.0-4.1.8.el5.x86_64.rpm           | 4.3 kB
00:00
(4/24): smbios-utils-2.2.27-3.2.el5.x86_64.rpm             |  13 kB
00:00
(5/24): dell_ie_tape_tandberg-1.1.0-7.i386.rpm             |  21 kB
00:00
(6/24): dell_ft_ie_interface-1.0.13-4.22.64.el5.noarch.rpm |  24 kB
00:00
(7/24): dell_ie_imc-1.0.0-4.4.288.el5.x86_64.rpm           |  28 kB
00:00
(8/24): dell_ie_bios-3.1.0-4.143.2.el5.x86_64.rpm          |  51 kB
00:00
(9/24): firmware-addon-dell-2.2.2-4.2.393.el5.x86_64.rpm   |  51 kB
00:00
(10/24): dell_ie_idrac7-2.0.0-4.10.1.el5.x86_64.rpm        |  58 kB
00:01
(11/24): dell_ie_nitrogen-2.0.0-4.22.1.el5.x86_64.rpm      |  58 kB
00:01
(12/24): smbios-utils-python-2.2.27-3.2.el5.x86_64.rpm     |  63 kB
00:01
(13/24): python-smbios-2.2.27-3.2.el5.x86_64.rpm           |  70 kB
00:01
(14/24): dell_ie_maser-3.2.0-4.28.2.el5.x86_64.rpm         | 115 kB
00:01
(15/24): dell_ie_tape_quantum-1.1.0-7.x86_64.rpm           | 120 kB
00:01
(16/24): libipmi0-1.0.0-4.4.2.el5.x86_64.rpm               | 129 kB
00:01
(17/24): dell_ie_tape_prostor-1.1.0-7.i386.rpm             | 168 kB
00:01
(18/24): python-ctypes-1.0.2-1.2.el5.x86_64.rpm            | 215 kB
00:04
(19/24): dell_ie_sas-3.2.0-4.2.2.el5.x86_64.rpm            | 217 kB
00:01
(20/24): firmware-tools-2.1.14-4.14.2.el5.noarch.rpm       | 221 kB
00:01
(21/24): dell_ie_tape_ibm-1.1.0-7.x86_64.rpm               | 482 kB
00:02
```

```
(22/24): libsmal0-3.1.0-4.142.1.el5.x86_64.rpm                                                  | 987 kB
00:05
(23/24): dell_ie_bp-1.1.0-7.i386.rpm                                                            | 1.5 MB     00:05
(24/24): dell_ie_bmc-1.1.0-7.i386.rpm                                                           | 1.5 MB     00:05
--------------------------------------------------------------------------------------------------------------------------------------------------------------
------
Total                                                                                 119 kB/s | 6.1 MB     00:52
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : libsmal0                                                                      1/24
  Installing     : dell_ie_maser                                                                 2/24
  Installing     : python-ctypes                                                                 3/24
  Installing     : libipmi0                                                                      4/24
  Installing     : python-smbios                                                                 5/24
  Installing     : firmware-tools                                                                6/24
  Installing     : smbios-utils-python                                                           7/24
  Installing     : smbios-utils                                                                  8/24
  Installing     : firmware-addon-dell                                                           9/24
  Installing     : dell_ft_ie_interface                                                         10/24
  Installing     : dell_ie_tape_quantum                                                         11/24
  Installing     : dell_ie_nitrogen                                                             12/24
  Installing     : dell_ie_imc                                                                  13/24
  Installing     : dell_ie_bios                                                                 14/24
  Installing     : dell_ie_idrac7                                                               15/24
  Installing     : dell_ie_tape_ibm                                                             16/24
  Installing     : dell_ie_sas                                                                  17/24
  Installing     : dell_ie_bp                                                                   18/24
  Installing     : dell_ie_tape_tandberg                                                        19/24
  Installing     : dell_ie_tape_prostor                                                         20/24
  Installing     : dell_ie_bmc                                                                  21/24
  Installing     : dell_ie_maser_inv_lcl                                                        22/24
  Installing     : dell_ie_rac_5                                                                23/24
  Installing     : dell_ft_install                                                              24/24

Installed:
  dell_ft_install.noarch 0:1.1-1

Dependency Installed:
  dell_ft_ie_interface.noarch 0:1.0.13-4.22.64.el5          dell_ie_bios.x86_64 0:3.1.0-4.143.2.el5          dell_ie_bmc.i386
0:1.1.0-7
  dell_ie_bp.i386 0:1.1.0-7                         dell_ie_idrac7.x86_64 0:2.0.0-4.10.1.el5          dell_ie_imc.x86_64
0:1.0.0-4.4.288.el5
  dell_ie_maser.x86_64 0:3.2.0-4.28.2.el5           dell_ie_maser_inv_lcl.x86_64 0:3.2.0-4.28.2.el5
dell_ie_nitrogen.x86_64 0:2.0.0-4.22.1.el5
  dell_ie_rac_5.x86_64 0:7.0.0-4.1.8.el5            dell_ie_sas.x86_64 0:3.2.0-4.2.2.el5             dell_ie_tape_ibm.x86_64
0:1.1.0-7
  dell_ie_tape_prostor.i386 0:1.1.0-7               dell_ie_tape_quantum.x86_64 0:1.1.0-7
dell_ie_tape_tandberg.i386 0:1.1.0-7
  firmware-addon-dell.x86_64 0:2.2.2-4.2.393.el5    firmware-tools.noarch 0:2.1.14-4.14.2.el5        libipmi0.x86_64
0:1.0.0-4.4.2.el5
  libsmal0.x86_64 0:3.1.0-4.142.1.el5               python-ctypes.x86_64 0:1.0.2-1.2.el5             python-smbios.x86_64
0:2.2.27-3.2.el5
  smbios-utils.x86_64 0:2.2.27-3.2.el5              smbios-utils-python.x86_64 0:2.2.27-3.2.el5

Complete!
```

Command 2 yum install $(bootstrap_firmware)

```
[14:38:42]# yum install $(bootstrap_firmware)
Invalid XML from module /usr/libexec/dell_dup/dell_ie_rac_5
Loaded plugins: security
dell-omsa-indep                                                                                                  | 1.9 kB     00:00
Setting up Install Process
No package pci_firmware(ven_0x8086_dev_0x25e4)/system(ven_0x1028_dev_0x01b3) available.
No package pci_firmware(ven_0x8086_dev_0x25e4) available.
….
….
Resolving Dependencies
--> Running transaction check
---> Package BMC_Firmware_componentid_05814_for_PowerEdge_1950.noarch 5:a14-1 set to be updated
---> Package Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3.noarch
5:a00-1 set to be updated
--> Processing Dependency: dell_ie_module(BROADCOM_FRMW) for package:
Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3
---> Package SAS_6_iR_Integrated_ven_0x1000_dev_0x0058_subven_0x1028_subdev_0x1f10_for_PowerEdge_1950.noarch
5:a04-1 set to be updated
---> Package Server_BIOS_componentid_00159_for_PowerEdge_1950.noarch 5:2.7.0-1 set to be updated
--> Running transaction check
---> Package dell_ie_nic_broadcom.x86_64 0:1.1.0-7 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================================================
Package                                                  Arch          Version          Repository                Size
================================================================================================================
================================================================================
Installing:
BMC_Firmware_componentid_05814_for_PowerEdge_1950                      noarch        5:a14-1
dell-omsa-indep          255 k
Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3        noarch
5:a00-1          dell-omsa-indep          4.2 M
SAS_6_iR_Integrated_ven_0x1000_dev_0x0058_subven_0x1028_subdev_0x1f10_for_PowerEdge_1950            noarch
5:a04-1          dell-omsa-indep          305 k
Server_BIOS_componentid_00159_for_PowerEdge_1950                       noarch        5:2.7.0-1
dell-omsa-indep          454 k
Installing for dependencies:
dell_ie_nic_broadcom                                     x86_64        1.1.0-7          dell-omsa-specific
1.5 M

Transaction Summary
================================================================================================================
================================================================================
Install       5 Package(s)
Upgrade       0 Package(s)

Total download size: 6.7 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): BMC_Firmware_componentid_05814_for_PowerEdge_1950-a14-1.noarch.rpm
| 255 kB     00:01
(2/5): SAS_6_iR_Integrated_ven_0x1000_dev_0x0058_subven_0x1028_subdev_0x1f10_for_PowerEdge_1950-a04-1.noarch.rpm
| 305 kB     00:01
(3/5): Server_BIOS_componentid_00159_for_PowerEdge_1950-2.7.0-1.noarch.rpm
```

| 454 kB   00:02
(4/5): dell_ie_nic_broadcom-1.1.0-7.x86_64.rpm | 1.5 MB
00:04
(5/5):
Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3-a00-1.noarch.rpm
| 4.2 MB   00:12

Total 301 kB/s | 6.7 MB   00:22
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
 Installing   : dell_ie_nic_broadcom 1/5
 Installing   : Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3
2/5
 Installing   : BMC_Firmware_componentid_05814_for_PowerEdge_1950
3/5
 Installing   : SAS_6_iR_Integrated_ven_0x1000_dev_0x0058_subven_0x1028_subdev_0x1f10_for_PowerEdge_1950
4/5
 Installing   : Server_BIOS_componentid_00159_for_PowerEdge_1950
5/5
Config does not specify automatic install during package install.
Please run update_firmware manually to install updates.
Config does not specify automatic install during package install.
Please run update_firmware manually to install updates.
Config does not specify automatic install during package install.
Please run update_firmware manually to install updates.
Config does not specify automatic install during package install.
Please run update_firmware manually to install updates.

Installed:
 BMC_Firmware_componentid_05814_for_PowerEdge_1950.noarch 5:a14-1
 Broadcom_NetXtreme_Gigabit_Network_Adapter_ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3.noarch 5:a00-1
 SAS_6_iR_Integrated_ven_0x1000_dev_0x0058_subven_0x1028_subdev_0x1f10_for_PowerEdge_1950.noarch 5:a04-1
 Server_BIOS_componentid_00159_for_PowerEdge_1950.noarch 5:2.7.0-1

Dependency Installed:
 dell_ie_nic_broadcom.x86_64 0:1.1.0-7

Complete!

Managing BIOS and firmware updates

Inventory firmware version levels

inventory_firmware

Usage

```
[15:11:46]# inventory_firmware
Wait while we inventory system:
Invalid XML from module /usr/libexec/dell_dup/dell_ie_rac_5
System inventory:
        System BIOS for PowerEdge 1950 = 2.3.1
        NetXtreme II BCM5708 Gigabit Ethernet rev 12 (ethGb1) = 4.0.3
        NetXtreme II BCM5708 Gigabit Ethernet rev 12 (ethGb2) = 4.0.3
```

```
        BIOS = xxxx
        BMC = 2.10
```

Compare versions installed to those available

```
update_firmware
```

Usage

```
[15:12:51]# update_firmware

Running system inventory...
Invalid XML from module /usr/libexec/dell_dup/dell_ie_rac_5

Searching storage directory for available BIOS updates...
Checking System BIOS for PowerEdge 1950 - 2.3.1
        Did not find a newer package to install that meets all installation checks.
Checking NetXtreme II BCM5708 Gigabit Ethernet rev 12 (ethGb1) - 4.0.3
        Available: pci_firmware(ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3) - 7.0.47
        Found Update: pci_firmware(ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3) - 7.0.47
Checking NetXtreme II BCM5708 Gigabit Ethernet rev 12 (ethGb2) - 4.0.3
        Available: pci_firmware(ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3) - 7.0.47
        Found Update: pci_firmware(ven_0x14e4_dev_0x164c_subven_0x1028_subdev_0x01b3) - 7.0.47
Checking BIOS - xxxx
        Available: dell_dup_componentid_00159 - 2.7.0
        Found Update: dell_dup_componentid_00159 - 2.7.0
Checking BMC - 2.10
        Available: dell_dup_componentid_05814 - 2.37
        Found Update: dell_dup_componentid_05814 - 2.37

Found firmware which needs to be updated.


Please run the program with the '--yes' switch to enable BIOS update.
  UPDATE NOT COMPLETED!
```

Install any applicable updates forcibly

```
update_firmware --yes
```

Providing System Information to API Support

If there is any issue with your system it is very important and as much information about the configuration of the the system is provided to API Support so that they can provide the correct help that you need.
To this end there is a simple command which can be run on the Appliance which will execute a number of debug command and collect the results in a zip file. This zip file can then be copied from the system and provided to API Support.

To use the command log in to the system as root and run:

```
# getinfo
```

The output will be something similar to:

```
# getinfo
Collecting command history...
Storing system files...
Executing debug commands...
Zipping the results...
A zip file of the system information has been saved in:
/opt/gateway/sysinfo/sysinfo_Appliance_1203081030.zip
#
```

Note: As referenced in this document earlier, it is also possible to carry out this command through the WAI.

Check Gateway Permission to Bind to Ports < 1024

The Gateway process should be able to run as an unprivileged user (admin) and still bind to privileged ports (ports < 1024). This is possible after a default install, but if the user has changed or modified their base gateway installation (perhaps even after installing a bespoke software patch) it may be possible that this functionality is broken.

To ensure that the Gateway process has the correct capability run:

```
# getcap /opt/gateway/platform/bin/vshell
```

The output of this command should be:

```
/opt/gateway/platform/bin/vshell = cap_net_bind_service+ep
```

If this is not the output received then execute the following to fix the capabilities:

```
# setcap 'cap_net_bind_service=+ep' /opt/gateway/platform/bin/vshell
```