KEMP Condor

Configuration Guide

VERSION: 1.2

UPDATED: FEBRUARY 2015

Copyright Notices

Table of Contents

1 Introduction

Condor is KEMP's multi-tenancy product. It is a product where multiple independent instances of the KEMP LoadMaster and GEO LoadMaster can operate. These instances can be referred to as tenants or Virtual Network Functions (VNFs).

Each LoadMaster instance within Condor can be deployed, stopped, started and updated at will.

1.1 Document Purpose

The purpose of this document is to describe the various options in the LoadMaster Condor Web User Interface (WUI).

For a high-level overview of the Condor product and architecture, refer to the **KEMP Condor, Product Overview**.

For instructional steps on how to perform certain tasks in the KEMP Condor, refer to the **Multi-Tenancy, Feature Description**.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in learning about the WUI options in the Condor product.

2 Multi-Tenancy Web User Interface (WUI) Options

The sections below describe the WUI options for the Condor.

2.1 Home

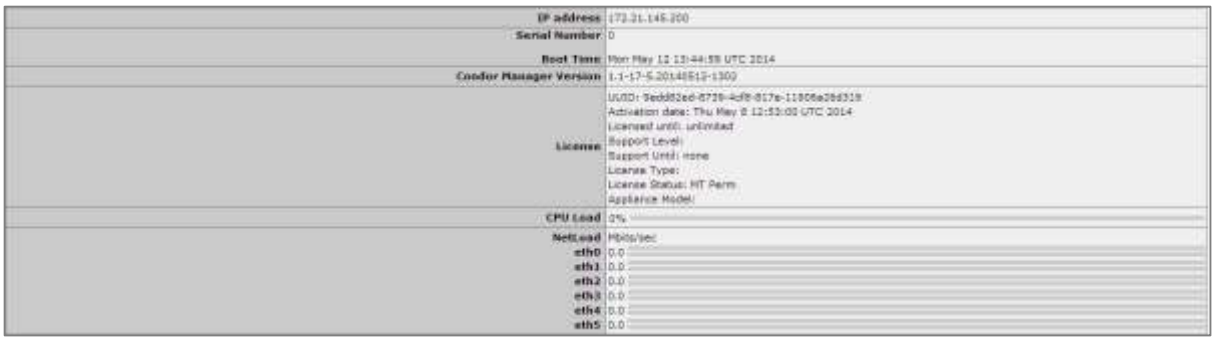

Figure 2-1: Home page

Clicking the **Home** menu option displays the home page which presents a list of basic information regarding the Condor.

The following information is displayed on this screen:

IP address: The IP address of the Condor

Serial Number: The serial number of the Condor

Boot Time: The time of the last server reboot

Condor Version: The firmware version of the Condor

License: License details are listed here, such as the activation date and end date of the Condor license

CPU Load: The percentage of load to the CPU of the Condor appliances

TPS [conn/s]: The total number of Transactions Per Second (TPS) and the number of Secure Sockets Layer (SSL) transactions per second

Net Load: The load of each configured interface.

2.2 Instance Management

This section is where the administration of installed Virtual Network Functions (VNFs) occurs.

2.2.1 VNF Status

This screen lists all the available VNFs and their status.

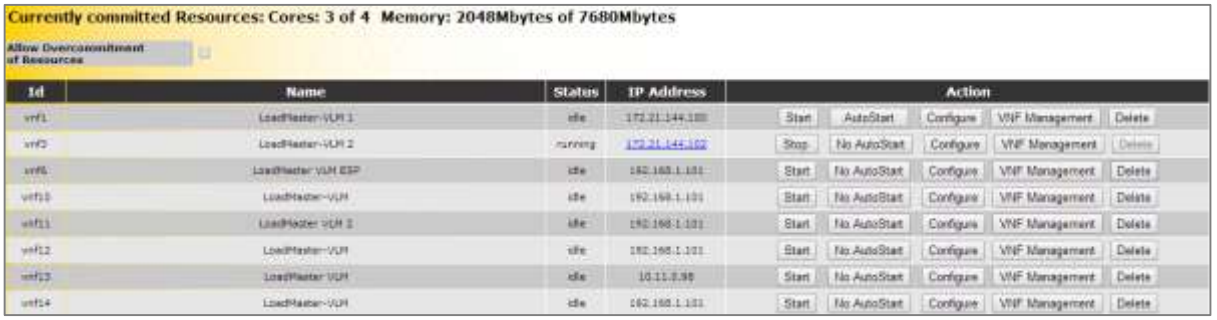

Figure 2-2: Status of Installed VNFs

At the top of the screen the currently committed resources are displayed, i.e. how many cores are in use and how much memory is currently in use.

Allow Overcommitment of Resources

Selecting this check box allows resources to be overcommitted. This can have an impact on performance.

> By default, Condor will only start running instances which do not exceed the total amount of available hardware resources.

A table is displayed which contains information and operations pertaining to each VNF. There are a number of columns in this table:

Id: A unique identifier for each VNF.

Name: A name to distinguish the VNF.

Status: The current status of the VNF.

IP Address: The IP address of the VNF. If the VNF is running, this will be displayed as a clickable hyperlink which will bring you to the VNF.

The last column contains a list of **Actions:**

- **Start:** Start this VNF.
- **AutoStart/No AutoStart:** Specify whether the system should auto-start this VNF upon reboot or not.
- **Configure:** Modify the settings for this VNF.
- **VNF Management:** Administer this VNF including deploying application templates.
- **Delete:** Delete this VNF.

2.2.1.1 Configure a VNF

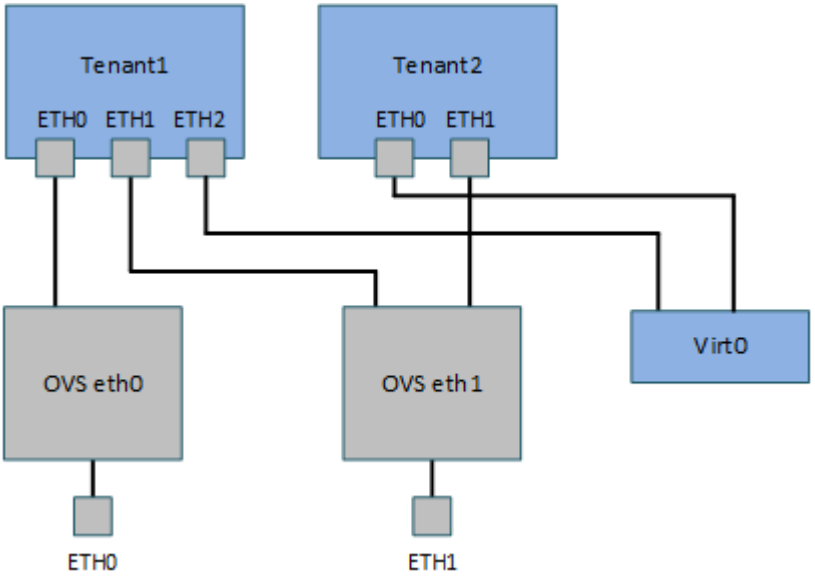

Figure 2-3: Multi-Tenancy Network Configuration

The Condor creates one Virtual-Switch per physical/VLAN interface. In addition, 10 host local networks are created. The tenant's vNICs connect either to one of these switches or to one of the host local networks. Each tenant can have up to 10 vNICs named **ETH0**… **9**.

Figure 2-4: Configure VNF

On this screen the VNF settings can be modified.

> The VNF has to be stopped in order to make changes on this screen. If the VNF has not been stopped, the fields on this screen will be greyed out. VNFs can be stopped on the **VNF Status** screen.

Name: The name of the VNF.

Memory: To select the amount of memory that the VNF uses.

CPUs: To select the number of CPUs that the VNF uses.

The second half of this screen lists the interfaces for this VNF along with related operations.

VNF Interface: The interface number.

MAC Address: The Media Access Control (MAC) address of the VNF.

Physical Interface/Virtual Network: To select either a physical interface or virtual network and select the relevant interface.

Add Interface: Adds the interface.

Delete Interface: Deletes the interface.

The interfaces can only be configured when the VNF is not running.

Reset: Resets all values.

Apply: Applies the changes to the VNFs.

2.2.1.2 Manage a VNF

Figure 2-5: Manage a VNF

Administrative functions can be performed to VNFs on this screen.

Backup VNF

Take a backup of the VNF.

Figure 2-6: Manage VNFs

Display Backups

Shows a list of previous backups for this VNF.

Restore: Restore the backup to the VNF.

Download: Downloads the backup to the local machine.

Delete: Deletes the backup.

Templates

A list of **Available Templates** is displayed on the left. Templates can be moved to the **Installed Templates** list on the right by selecting them and clicking the right arrow. To remove templates, use the left arrow. Click **Install Templates** to apply the changes to the VNF.

2.2.2 Package Management

Import VNF Package

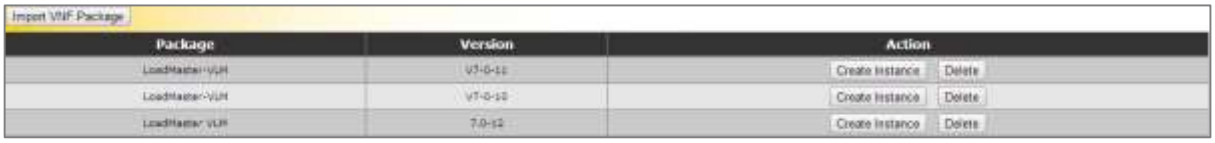

Figure 2-7: Install VNF Packages

Import a new VNF package.

Package: The name of the VNF package.

Version: The VNF package version.

Action:

- **Create Instance:** Create an instance of this template.

> When creating an instance the package needs to be decompressed. It can take approximately 10 minutes for an instance to be created.

- **Delete:** Delete this template.

2.2.2.1 Create a VNF Instance

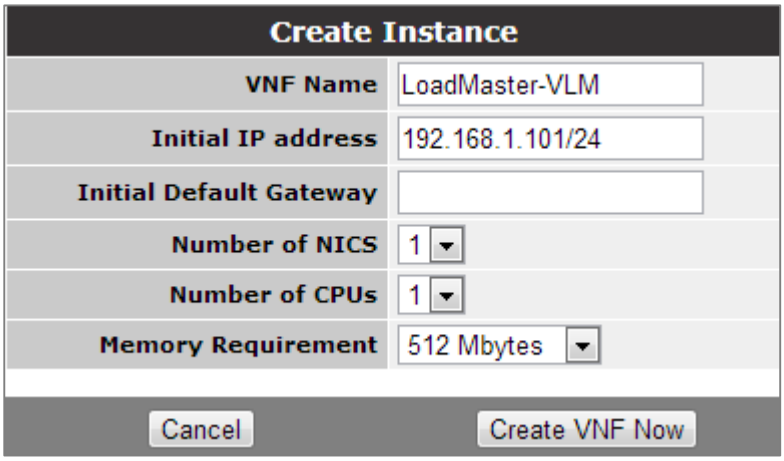

Figure 2-8: Create Instance

VNF Name: Specify the name of the VNF.

Initial IP address: Enter the initial IP address of the VNF.

Initial Default Gateway: Enter the initial default gateway of the VNF.

Number of NICS: Select the number of Network Interface Console (NICs).

Number of CPUs: Select the number of CPUs.

Memory Requirement: Select the amount of memory required for this VNF.

Create VNF Now: Creates an instance of this VNF.

2.2.3 Manage Templates

Application templates make the setting up of Virtual Services easier by automatically configuring the parameters for a Virtual Service. Before a template can be used to configure a Virtual Service, it must be imported and installed on the Condor or a tenant LoadMaster.

Templates can be downloaded from www.kemptechnologies.com.

Figure 2-9: Manage Templates

Click the **Choose File** button, select the template you wish to install and click the **Add New Template** button to install the selected template. This template then needs to be assigned to the VNF in the **Manage VNF** screen before it becomes available for use in the tenant LoadMaster. Refer to **Section 2.2.1.2** for more information..

Click the **Delete** button to remove the template.

For details on how to use a template to create and configure a new Virtual Service and where to obtain templates, please refer to the **Virtual Services and Templates, Feature Description** document.

2.3 Statistics

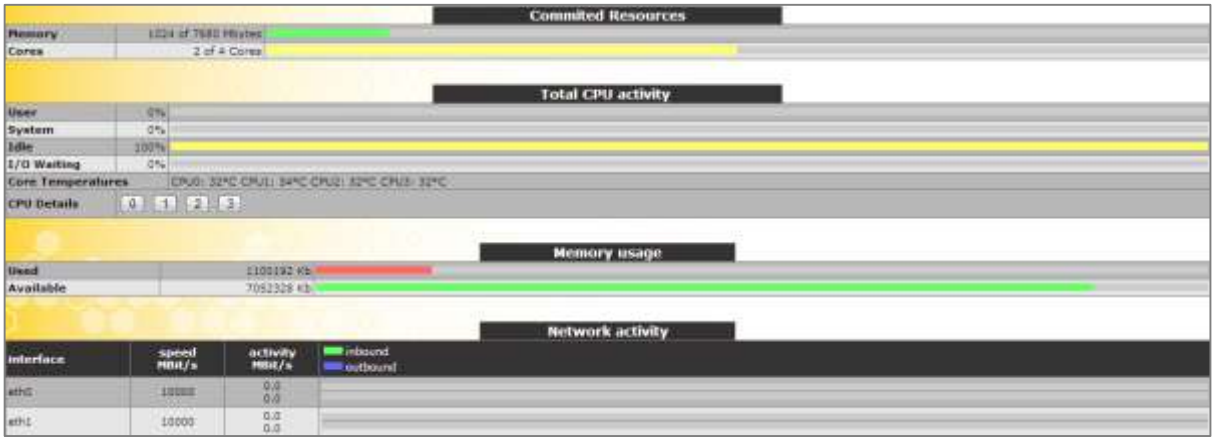

Figure 2-10: Statistics

The **Statistics** screen displays the activity and resources used of the Condor.

2.3.1.1 Committed Resources

Memory: The amount of total memory used.

Cores: The number of processor cores in use.

2.3.1.2 Total CPU activity

This table displays the following CPU utilization information for a given Condor:

Statistic	Description
User	The percentage of the CPU spent processing in user mode
System	The percentage of the CPU spent processing in system mode
Idle	The percentage of CPU which is idle
I/O Waiting	The percentage of the CPU spent waiting for I/O to complete

The sum of these 4 percentages will equal 100%.

Core Temp: The temperature for each CPU core is displayed for Condor hardware appliances. Temperature will not show on a virtual statistics screen.

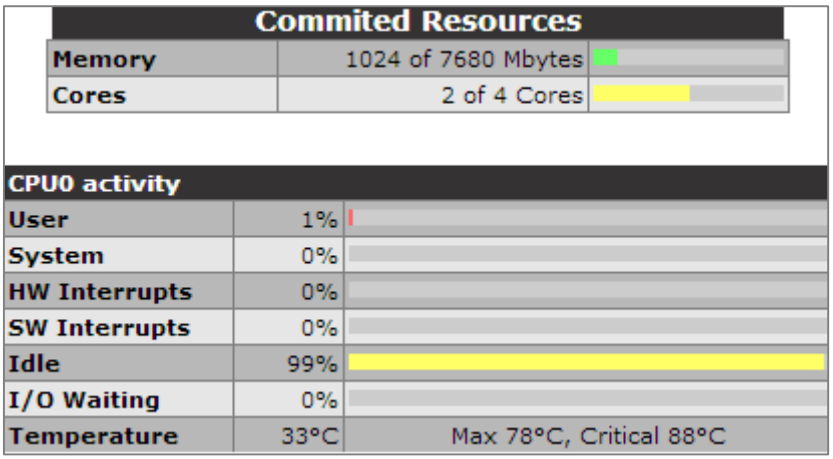

Figure 2-11: CPU Details

CPU Details: The number buttons can be clicked in the **CPU Details** row to get more detailed statistics on each CPU.

Memory usage

This bar graph shows the amount of memory in use and the amount of memory free.

Network activity

These bar graphs show the current network throughput on each interface.

2.4 System Configuration

2.4.1 Interfaces

Describes the external network and internal network interfaces. The screen has the same information for the **eth0** and **eth1** Ethernet ports.

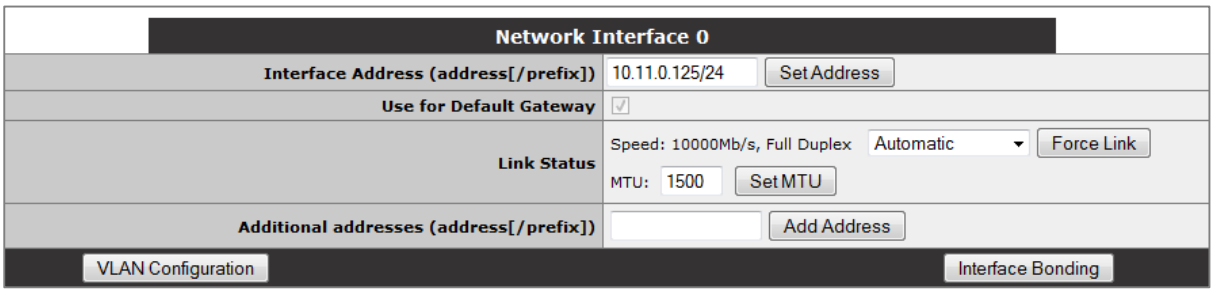

Figure 2-12: Network Interface options

Within the **Interface Address (address[/prefix])** text box you can specify the Internet address of this interface.

By default, the **Speed** of the link is automatically detected. In certain configurations, this speed is incorrect and must be forced to a specific value.

The **Use for Default Gateway** check box is only available if the **Enable Alternate GW support** is selected in the **Network Options** screen. If the settings being viewed are for the default interface this option will be greyed out and selected. To enable this option on another interface, go to the other interface by clicking it in the main menu on the left. Then this option is available to select.

Within the **MTU** field you can specify the maximum size of Ethernet frames that will be sent from this interface. The valid range is **512** - **9216**.

> The valid range of **512 - 9216** may not apply to VLMs as the range will be dependent on the hardware the VLM is running on. It is advised to check your hardware restrictions for supported MTU sizes.

Using the **Additional addresses** field allows the Condor to give multiple addresses to each interface, as aliases. This is sometimes referred to as a "router on a stick". It allows both IPv4 and IPv6 addresses in standard IP+CIDR format, so this can also be used to do a mixed mode of IPv4 and IPv6 addresses on the same interface. Any of the subnets that are added here will be available for both virtual IPs and real server IPs.

Creating a Bond/Team

Before creating a bonded interface please note the following:

- You can only bond interfaces higher than the parent, so if you choose to start with port 10 then you can only add ports 11 and greater

- Bond links first if you need VLAN tagging then add VLANs after the bond has been configured
- In order to add a link to a bonded interface, any IP addressing must first be removed from the link to be added
- Enabling the Active-Backup mode generally does not require switch intervention
- Bonding **eth0** with **eth1** can lead to serious issues and is not allowed to occur

Click the **Interface Bonding** button to request the bond.

Confirm the bond creation by clicking the **Create a bonded interface** button.

Acknowledge the warning dialogs.

Using the Web User Interface (WUI) select the **System Configuration > Interfaces > bndx** menu option.

If you do not see the **bndX** interface, refresh your browser, then select the bonded interface and click the **Bonded Devices** button.

Select the desired bonding mode.

Add the additional interfaces to this bond.

Configure the IP and Subnet Mask on the bonded interface.

Removing a Bond/Team

Remove all VLANs on the bonded interface first; if you do not remove them they will automatically be assigned to the physical port at which the bond started.

Select the **System Configuration > Interfaces > bndx** menu option. If you do not see the **bndX** interface refresh your browser, then select the bonded interface, then click the **Bonded Devices** button.

Unbind each port by clicking the **Unbind Port** button, repeat until all ports have been removed from bond.

Once all child ports have been unbounded, you can unbond the parent port by clicking **Unbond this interface** button.

Adding a VLAN

Select the interface and then select the **VLAN Configuration** button.

Figure 2-13: VLAN Id

Add the **VLAN Id** value and select the **Add New VLAN** menu option.

Repeat as needed. To view the VLANs, select the **System Configuration > Interfaces** menu option.

Removing a VLAN

To remove a VLAN select the **System Configuration > Interfaces** menu option and select the appropriate VLAN ID from the drop-down list.

Once selected, delete the IP and then click **Set Address**. Once the IP has been removed you will have the option to delete the VLAN, by clicking the **Delete this VLAN** button.

Repeat as needed. To view the VLANs select the **System Configuration > Interfaces** menu option and select the appropriate VLAN ID from the drop-down list.

2.4.2 Local DNS Configuration

2.4.2.1 Hostname Configuration

Figure 2-14: Set Hostname

Set the hostname of the local machine by entering the hostname in the **Current Hostname** text box and clicking the **Set Hostname** button. Only alphanumeric characters are allowed.

2.4.2.2 DNS Configuration

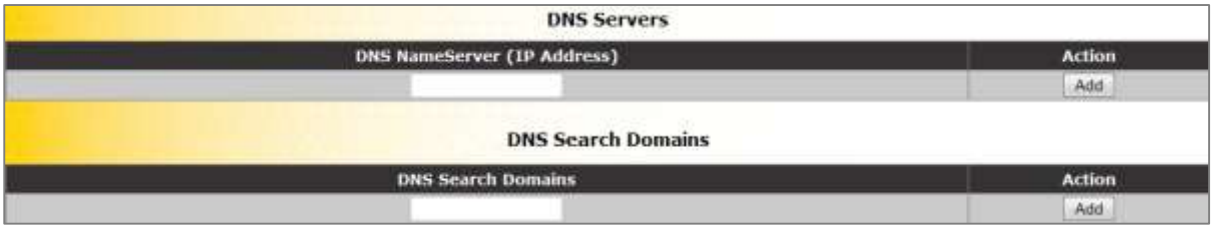

Figure 2-15: DNS Configuration

DNS NameServer (IP Address)

Enter the IP address of a DNS server that will be used to resolve names locally on the Condor in this field and click the **Add** button. A maximum of three DNS servers are allowed.

DNS Search Domains

Specify the domain name that is to be prepended to requests to the DNS Name Server in this field and click the **Add** button. A maximum of six Search Domains are allowed.

2.4.3 Route Management

This option permits the configuration of default and static routes.

2.4.3.1 Default Gateway

The LoadMaster requires a default gateway through which it can communicate with the Internet.

Figure 2-16: Default Gateway

If both IPv4 and IPv6 addresses are being used on the Condor, then both an IPv4 and IPv6 Default Gateway Address are required.

IPv4 and IPv6 default gateways must be on the same interface.

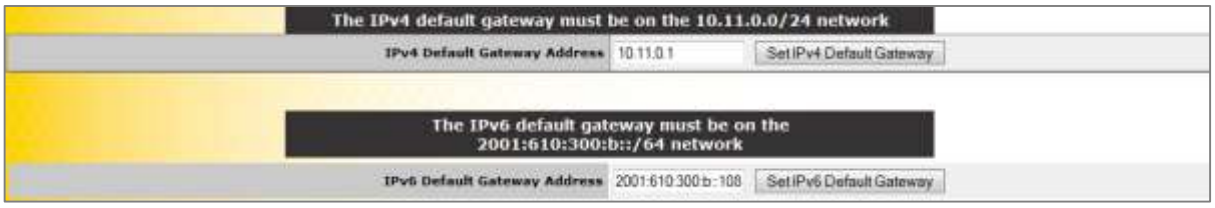

Figure 2-17: IPv4 and IPv6 addresses

2.4.3.2 Additional Routes

Figure 2-18: Additional Routes

Further routes can be added. These routes are static and the gateways must be on the same network as the Condor.

2.4.4 Access Control

2.4.4.1 Packet Filter

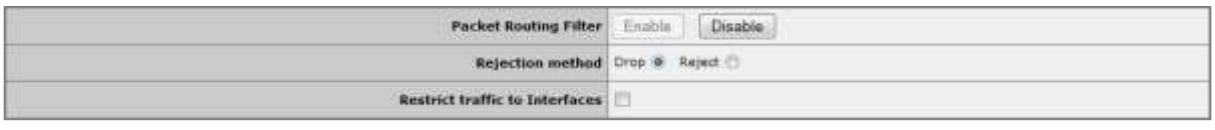

Figure 2-19: Packet Filter

Packet Routing Filter

The **Packet Routing Filter** can be enabled or disabled here. If the **Packet Routing Filter** is enabled, all unknown traffic will be ignored. You can select whether to **Drop** or **Reject** this unknown traffic.

Reject/Drop blocked packets

When an IP packet is received from a host, which is blocked using the Access Control Lists (ACLs), the request is normally ignored (dropped). The Condor may be configured to return an ICMP reject packet, but for security reasons it is usually best to drop any blocked packets silently.

Restrict traffic to Interfaces

This setting enforces restrictions upon routing between attached subnets.

2.4.4.2 Access Lists

Condor supports a "blacklist" Access Control List (ACL) system. Any host or network entered into the ACL will be blocked from accessing any service provided by the Condor.

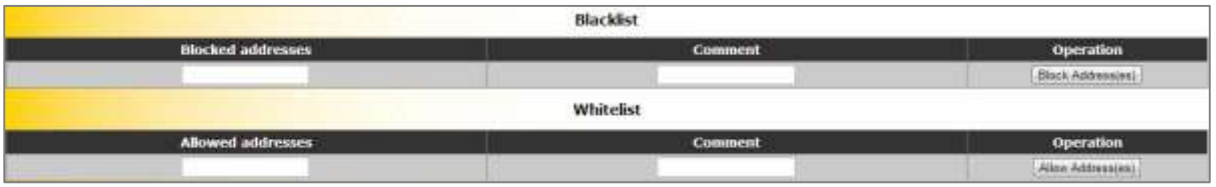

Figure 2-20: Access Lists

The ACL is only enabled when the Packet Filter is enabled. The whitelist allows a specific IP address or address range access. If the address or range is part of a larger range in the blacklist, the whitelist will take precedence for the specified addresses.

If a user does not have any addresses listed in their blacklist and only has addresses listed in their whitelist, then only connections from addresses listed on the whitelist are allowed and connections from all other addresses are blocked.

This option allows a user to add or delete a host or network IP address to the Access Control List. In addition to IPv4 addresses - IPv6 addresses are allowed in the lists if the system is configured with an IPv6 address family. Using a network specifier specifies a network.

For example, specifying the address **192.168.200.0/24** in the blacklist will block all hosts on the 192.168.200 network.

2.4.5 System Administration

These options control the base-level operation of the Condor. Many of these options will require a system reboot.

2.4.5.1 User Management

Figure 2-21: User Management

The User Management screen allows you to:

- Change the appliance password
- Change an existing user's password by clicking the **Password** button in the **Action** section
- Add a new user and associated password
- Change the permissions for an existing user by clicking the **Modify** button in the **Action** section

User names can contain alphanumeric characters and periods and dashes ('**.**' and '**_**').

The **Use RADIUS Server** option allows you to determine whether the user will use RADIUS server authentication or not when logging on to the Condor. The RADIUS Server details must be set up before this option can be used.

RADIUS server can be used to authenticate users who wish to log on to the Condor. Condor passes the user's details to the RADIUS server and the RADIUS server informs Condor whether the user is authenticated or not.

When Session Management is enabled, the Use RADIUS Server option is not available within this screen.

Figure 2-22: Permissions

In this screen you may set the level of user permissions. This determines what configuration changes the user is allowed to perform. The primary user, bal, always has full permissions. Secondary users may be restricted to certain functions.

Named users, even those without User Administration privileges, can change their own passwords. When a named user clicks the **System Administration > User Management** menu option the **Change Password** screen appears.

Figure 2-23: Change Password

From within this screen, users can change their own password. Once changed, a confirmation screen appears after which the users will be forced to log back in to Condor using their new password.

2.4.6 Update License

Figure 2-24: Update License

This screen displays the activation date and the expiration date of the current license. Before updating the license in the Condor, you must either contact your KEMP representative or use the **Upgrade** option. After you have contacted KEMP or used the **Upgrade** option, there are two ways to upgrade a license – via the Online method and via the Offline method. For more information and instructions, refer to the **Licensing, Feature Description**. A reboot may be required depending on which license you are applying.

Licensing is done in the Condor and is based on the maximum number of tenants that can be started. This means that the LoadMaster tenants do not need to be licensed individually. There are three different multi-tenancy license types available which provide a different number of maximum tenants – 10, 20 and 30. 10 is number of tenants for the default Condor license.

The **Update License** option is not available in tenant LoadMasters that were deployed using the KEMP Condor product. This is because licensing is controlled at the Condor-level.

2.4.7 System Reboot

Figure 2-25: System Reboot

Reboot

Reboot the appliance.

Shutdown

Clicking this button attempts to power down the Condor. If, for some reason, the power down fails, it will at a minimum halt the CPU.

Reset Machine

Reset the configuration of the appliance with the exception of the license and username and password information.

2.4.8 Update Software

Figure 2-26: Update Software

Contact support to obtain the location of firmware patches and upgrades. Firmware downloads require Internet access. Detailed patch information is available at http://forums.kemptechnologies.com/

Update Machine

Once you have downloaded the firmware you can browse to the file and upload the firmware directly into the Condor. The firmware will be unpacked and validated on the Condor. If the patch is validated successfully you will be ask to confirm the release information. To complete the update you will need to reboot the appliance. This reboot can be deferred if needed.

Restore Software

If you have completed an update of the Condor firmware you can use this option to revert to the previous build.

2.4.9 Backup and Restore

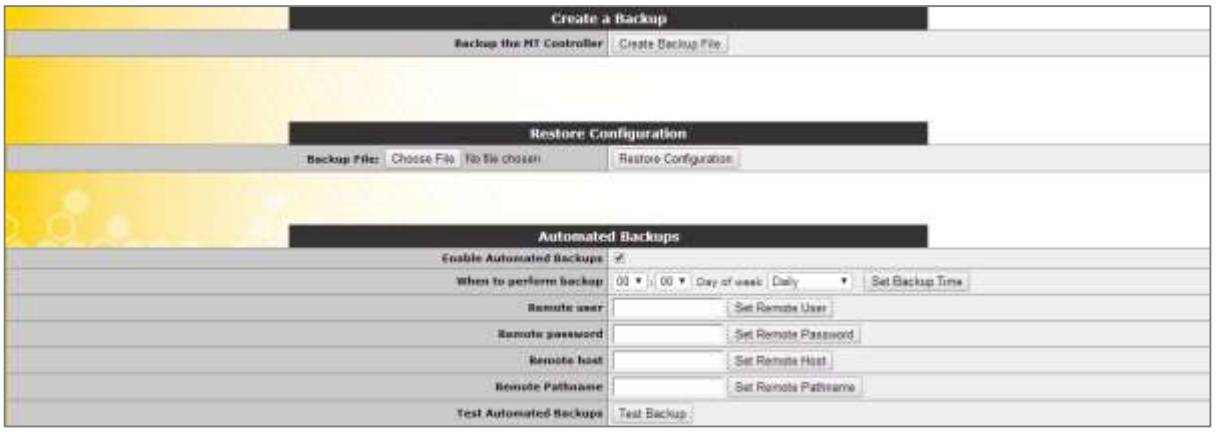

Figure 2-27: Backup and Restore

Create Backup File

Generate a backup of the Condor. License information and SSL Certificate information is not contained in the backup.

Restore Configuration

Browse to and restore a Condor backup file.

Automated Backups

If the **Enable Automated Backups** check box is selected, the system may be configured to perform automated backups on a daily or weekly basis.

When to perform backup

Specify the time (24 hour clock) of backup. Also select whether to backup daily or on a specific day of the week. When ready, click the **Set Backup Time** button.

Remote user

Set the username required to access remote host.

Remote password

Set the password required to access remote host.

Remote host

Set the remote host name.

Remote Pathname

Set the location on the remote host to store the file.

Test Automated Backups

Clicking the **Test Backup** button performs a test to check if the automated backup configuration is working correctly. The results of the test can be viewed within the System Message File.

The Automated Backup transfer protocol is currently FTP only.

2.4.10 Date/Time

You can manually configure the date and time of the Condor or leverage a Network Time Protocol (NTP) server.

Figure 2-28: Set Date and Time

NTP host(s)

Specify the host which is to be used as the NTP server.

The time zone must always be set manually.

2.4.11 Logging Options

2.4.11.1 System Log Files

Figure 2-29: Log Files

Boot.msg File: Contains information, including the current version, during the initial starting of the Condor.

Warning Message File: Contains warnings logged during the operation of the Condor.

System Message File: Contains system events logged during the operation of Condor. This includes both operating system-level and Condor internal events.

Reset Logs: This will reset all log files.

Save all System Log Files: This saves the files to your computer. It can be useful to send log files to KEMP support when troubleshooting an issue.

2.4.11.1.1 Debug Options

The Condor has a range of features that will help you and KEMP Support staff with diagnosing connectivity issues. Clicking the **Debug Options** button will bring up the screen shown below.

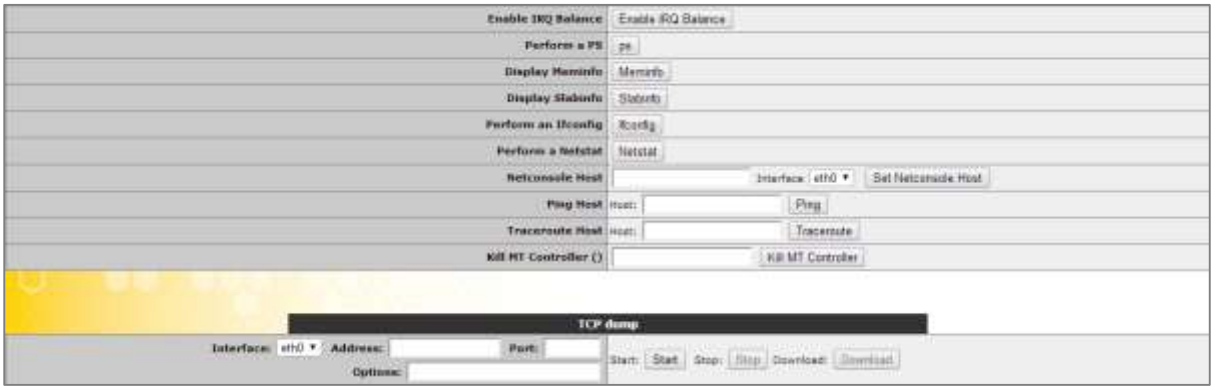

Figure 2-30: Debug Options

Enable IRQ Balance: Enable this option only after consulting with KEMP support staff.

Perform a PS: Performs a ps on the system.

Display Meminfo: Displays raw memory statistics.

Display Slabinfo: Displays raw slab statistics.

Perform an Ifconfig: Displays raw Ifconfig output.

Perform a Netstat: Displays Netstat output.

Netconsole Host: The syslog daemon on the specified host will receive all critical kernel messages. The syslog server must be on the local LAN and the messages sent are UDP messages.

You can select which interface the Netconsole Host is set to via the **Interface** dropdown.

Please ensure that the netconsole host specified is on the selected interface as errors may occur if it is not.

Ping Host: Performs a ping on the specified host.

Traceroute Host: Perform a traceroute of a specific host.

Kill MT Console (): Permanently disables all Condor functions. The Condor can be re-enabled by being relicensed.

Please do not kill your Condor without consulting KEMP Technical Support first.

TCP dump

A TCP dump can be captured either by one or all Ethernet ports. Address and port parameters, as well as optional parameters may be specified. The maximum number of characters permitted in the optional field is **255**.

You can stop and start the dump. You can also download it to a particular location.

2.4.11.2 Syslog Options

The Condor can produce various warning and error messages using the syslog protocol. These messages are normally stored locally.

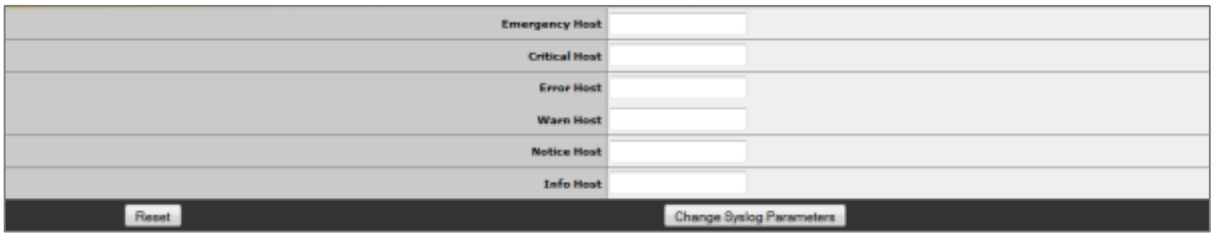

Figure 2-31: Syslog Options

It is also possible to configure the Condor to transmit these error messages to a remote syslog server by entering the relevant IP address in the relevant text box and clicking **Change Syslog Parameters**.

Six different error message levels are defined and each message level may be sent to a different server. Notice messages are sent for information only; emergency messages normally require immediate user action.

Examples of the type of message that may be seen after setting up a Syslog server are below:

- **Emergency**: Kernel-critical error messages
- **Critical**: Unit has failed
- **Error**: Authentication failure for root from 192.168.1.1
- **Warn**: Interface is up/down
- **Notice**: Time has been synced
- **Info**: Local advertised Ethernet address

One point to note about syslog messages is they are cascading in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels above WARN but none for levels below WARN.

We recommend you do not set all six levels for the same host because multiple messages for the same error will be sent to the same host.

To enable a syslog process on a remote Linux server to receive syslog messages from the Condor, the syslog must be started with the "-r" flag.

2.4.11.3 SNMP Options

With this menu, the SNMP configuration can be modified.

Figure 2-32: SNMP Options

Enable SNMP

This check box enables or disables SNMP metrics. For example, this option allows the Condor to respond to SNMP requests.

By default SNMP is disabled.

When the feature is enabled, the following traps are generated:

- **ColdStart**: generic (start/stop of SNMP sub-system)
- **VsStateChange**: (Virtual Service state change)
- **RsStateChange:** (Real Server state change)

The information regarding all Condor-specific data objects is stored in three enterprise-specific MIBs (Management Information Base).

ONE4NET-MIB.txt	enterprise id
IPVS-MIB.txt	Virtual Server stats
B-100-MIB.txt	Condorconfiguration data

These MIBs (which can be found on the Condor CD) need to be installed on the SNMP manager machine in order to be able to request the performance-/config-data of the Condor via SNMP.

The description of the counters can be taken from the Condor MIBs (the description clause). Apart from just reading the MIB this can be done for Linux (nad ucdsnmp) with the command:

snmptranslate -Td -OS <oid>

where <oid> is the object identifier in question.

Example: <oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

snmptranslate -Td –Ov .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

.1.3.6.1.4.1.12196.12.2.1.12

RSConns OBJECT-TYPE

-- FROM **IPVS-MIB**

SYNTAX **Counter32**

MAX-ACCESS **ead-only**

STATUS **current**

DESCRIPTION **"the total number of connections for this RS"**

::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2) rsEntry(1) 12 }

The data object defined in the Condor MIBS is a superset to the counters displayed by the WUI.

> The data objects on the Condor are not writable, so only GET requests (GET, GET-NEXT, GET-BULK etc.) should be used.

Configure SNMP Clients

With this option, the user can specify from which SNMP management hosts the Condor will respond to.

> If no client has been specified, the Condor will respond to SNMP management requests from any host.

Configure SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Allowed characters in the **Community String** are as follows: **a**-**z**, **A**-**Z**, **0**-**9**, **_.-@()?#%^+~!**.

Configure SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the Condor.

Configure SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a Condor, a Virtual Service or a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.

> SNMP traps are disabled by default.

Configure SNMP Trap Sink1

This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

Configure SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

2.4.11.4 Email Options

This screen permits the configuration of email alerting for Condor events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided.

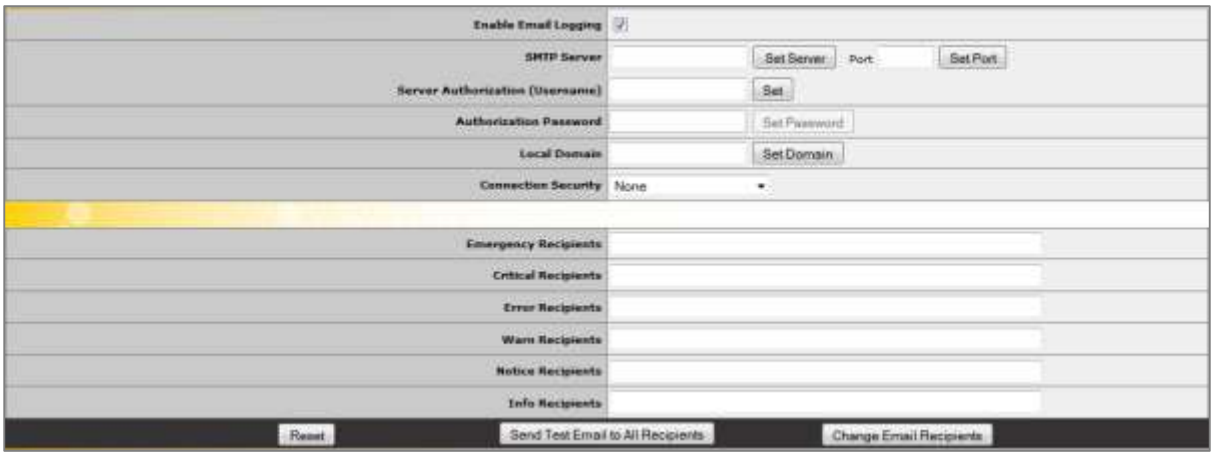

Figure 2-33: Email Options

Figure 2-34: Sample email alert

SMTP Server

Enter the FQDN or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

Port

Specify the port of the SMTP server which will handle the email events.

Server Authorization (Username)

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Authorization Password

Enter the password if your mail server requires authorization for mail delivery. This is not a required if you mail server does not require authorization.

Local Domain

Enter the top-level domain, if your mail server is part of a domain. This is not a required parameter.

Connection Security

Select the type of security for the connection;

- None
- STARTTLS, if available
- STARTTLS
- SSL/TLS

Set Email Recipient

In the various **Recipients** text boxes, enter the email address that corresponds with the level of notification desired. Multiple email addresses are supported by a comma-separated list, such as:

Info Recipients: **info@kemptechnologies.com, sales@kemptechnologies.com**

Error Recipients: **support@kemptechnologies.com**

Clicking the **Send Test Email to All Recipients** button sends a test email to all the listed email recipients.

2.4.12 Miscellaneous Options

2.4.12.1 WUI Settings

Only the **bal** user or users with 'All Permissions' set can use this functionality. Users with different permissions can view the screen but all buttons and input fields are greyed out.

Figure 2-35: WUI Settings

Enable Hover Help

Enables blue hover notes shown when the pointer is held over certain fields.

Message of the Day (MOTD)

Type in text into the field and click the **Set MotD** button. This message will be displayed within the Condor home screen.

The maximum allowed message length is 5,000 characters. HTML is supported, but not required.

Set Statistics Display Size

This sets the maximum number of rows that can be displayed in the Statistics page. The allowable range is between 10 and 100 rows being displayed on the page.

End User License

Click the **Show EULA** button to display the Condor End User License Agreement.

2.4.12.2 WUI Session Management

Only the **bal** user or users with 'All Permissions' can use this functionality, but only the **bal** user can enable or disable Session Management. Users with 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out. All other users cannot view this portion of the screen.

When WUI Session Management is enabled, there are two levels of authentication enforced in order to access the Condor WUI. The initial level is Basic Authentication where users login using the **bal** or **user** logins, which are usernames defined by the system.

Once logged in via Basic Authentication, the user then must log in using their local username and password to begin the session.

Basic Authentication Password

The Basic Authentication Password must be set before WUI Session Management can be enabled.

The Basic Authentication password for the **user** login can be set by typing the password into the **Basic Authentication** field and clicking the **Set Basic Password** button.

The password needs to be at least 8 characters long and should be a mix of alpha and numeric characters. If the password is considered to be too weak, a message appears asking you to enter a new password.

Only the **bal** user is permitted to set the Basic Authentication password.

Once the password is set for the first time the **Enable Session Management** option appears.

Figure 2-36: WUI Session Management

Enable Session Management

Selecting the **Enable Session Management** check box enables the WUI Session Management functionality. This will force all users to initially log in to the server using either the **bal** or **user** logins and then to login to the session using their normal credentials.

When this check box is selected, the user is required to log in to use the Condor.

LDAP users need to login using the full domain name. For example an LDAP username should be **test@kemp.com** and not just **test**.

Figure 2-37: User Credentials

Once the WUI Session Management functionality is enabled, all the WUI Session Management options appear.

Figure 2-38: WUI Session Management

Basic Authentication Password

The Basic Authentication password for the **user** login can be set by typing the password into the **Basic Authentication Password** text box and clicking the **Set Basic Password** button.

The password needs to be at least 8 characters long and should be a mix of alpha and numeric characters. If the password is considered to be too weak, a message appears asking you to enter a new password.

Failed Login Attempts

The number of times that a user can fail to login correctly before they are blocked can be specified within this text box. The valid values that may be entered are numbers between **1** and **999**.

If a user is blocked, only the **bal** user or other users with **All Permissions** set can unblock a blocked user.

If the **bal** user is blocked, there is a 'cool-down' period of ten minutes before the **bal** user can login again.

Idle Session Timeout

The length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session. The valid values that may be entered are numbers between **60** and **86400** (between one minute and 24 hours).

2.4.11.1.2 Active and Blocked Users

Only the **bal** user or users with 'All Permissions' set can use this functionality. Users with 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out. All other users cannot view this portion of the screen.

Figure 2-39: Currently Active Users

Currently Active Users

The user name and login time of all users logged into the Condor are listed in this section.

To immediately log out a user and force them to log back into the system, click the **Force logout** button.

To immediately log out a user and to block them from being able to log in to the system, click the **Block user** button**.** The user will not be able to log back in to the system until they are unblocked or until the Condor reboots. Clicking the **Block user** button does not force the user to log off; to do this, click the **Force logout** button.

If a user exits the browser without logging off, that session will remain open in the currently active users list until the timeout has reached. If the same user logs in again, before the timeout is reached, it would be within a separate session.

Currently Blocked Users

The user name and login time of when the user was blocked are listed within this section.

To unblock a user to allow them to log in to the system, click the **Unblock** button.

2.4.12.3 Remote Access

Figure 2-40: Remote Access

Allow Remote SSH Access

You can limit the network from which clients can connect to the SSH administrative interface on Condor.

Using

Specify which addresses that remote administrative SSH access to the Condor is allowed.

Port

Specify the port used to access the Condor via the SSH protocol.

Disable SSH-V1 Prot

Select to disable the SSH-V1 protocol. This is recommended by KEMP. The Condor supports the SSH-V1 protocol for backwards compatibility with older software versions.

Allow Web Administrative Access

Selecting this check box allows administrative web access to the Condor. Disabling this option will stop access upon the next reboot.

> Disabling web access is not recommended.

Using

Specify the addresses that administrative web access is to be permitted.

Port

Specify the port used to access the administrative web interface.

Administrative Default Gateway

When administering the Condor from a non-default interface, this option allows the user to specify a different default gateway for administrative traffic only.

> If the **Administrative Default Gateway** is being changed to another interface that is not accessible without proper routing, a static route into the Condor should be added before changing the administrative interface IP. Once the routing is in please, the interface can be switched and the administrative default gateway can be selected if required. Then the static route can be removed.

RADIUS Server

Here you can enter the address of the RADIUS server that is to be used to validate user access to the Condor. To use RADIUS server you have to specify the **Shared Secret**.

A shared secret is a text string that serves as a password between the Condor and the RADIUS server.

The **Revalidation Interval** specifies how often a user should be revalidated by the RADIUS server.

Below is an example of the configuration that needs to be on the radius server for authorization to work.

> The below example is for Linux only.

The Reply-Message should be self-explanatory on what permission it is allowing. They should match up to the user permissions page in the WUI, with the exception of “All Permissions”:

LMUSER Cleartext-Password := "1fourall"

Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users"

Enable API Interface

Enables/disables the RESTful Application Program Interface (API).

2.4.12.4 Network Options

Figure 2-41: Network Options

Enable Server NAT

This option enables Network Address Translation (NAT) globally.

Enable Alternate GW support

If there is more than one interface enabled, this option provides the ability to move the default gateway to a different interface.

Enabling this option adds another option to the **Interfaces** screen – **Use for Default Gateway**.

Enable Strict IP Routing

When this option is selected, only packets which arrive at the machine over the same interface as the outbound interface are accepted.

SDN Controller

Specify the address of the Software-Defined Networking (SDN) Console.

References

Unless otherwise specified, the following documents can be found at http://www.kemptechnologies.com/documentation.

Licensing, Feature Description

Virtual Services and Templates, Feature Description

Multi-Tenancy, Feature Description

KEMP Condor, Product Overview

Web User Interface, Configuration Guide

Document History

Date	Change	Reason for Change	Version	Resp.
Apr 2014	Initial draft	First draft of document	1.0	LB
May 2014	Release updates	Updates for MT_1.1-16	1.1	LB
Feb 2015	Release updates	Updates for 7.1-24a	1.2	LB

