DNS & DHCP Activity Monitor
Installation & User Guide

Version: 2.2.1 2012-02-23 Rev A

Every effort has been taken to ensure the accuracy of this manual but Accumuli Security Ltd. is not responsible for typographical errors or inconsistencies that arise due to the ongoing improvement and maintenance of the product. This manual does not form part of a contract.

Company and product names mentioned are the trademarks of their respective owners. Mentions of these are for information only. Accumuli Security Ltd. accepts no responsibility for the performance or use of these products except where they are supplied as a fully integrated part of this product. Some parts of this product are licensed from third parties and no rights to use these products other than as an integral part of this product are granted.

Contents

Chapter

1

1 Introduction

1.1 Overview

Accumuli Security DNS and DHCP Activity Monitor (DDAM) logs DNS and DHCP activity from DNS and DHCP Servers and concentrates the information from one or more servers to a central location.

DDAM can monitor DNS and DHCP activity and alert on specific conditions. DDAM also generates report data that can be analyzed for different time periods.

DDAM allows reports to be scheduled on a recurring basis and published as PDF (Portable Document Format) files that can be emailed to individual users. The contents of each PDF report can also be customized so that only the relevant information is reported.

1.2 Master, Collectors, Nodes and Collection Methods

DDAM utilizes a distributed collection architecture. All application data is concentrated and stored on a Master server, this is also referred to as the "DDAM Master" or "DDAM Master Server".

When backing up and restoring all DDAM application data, only the Master server need be considered.

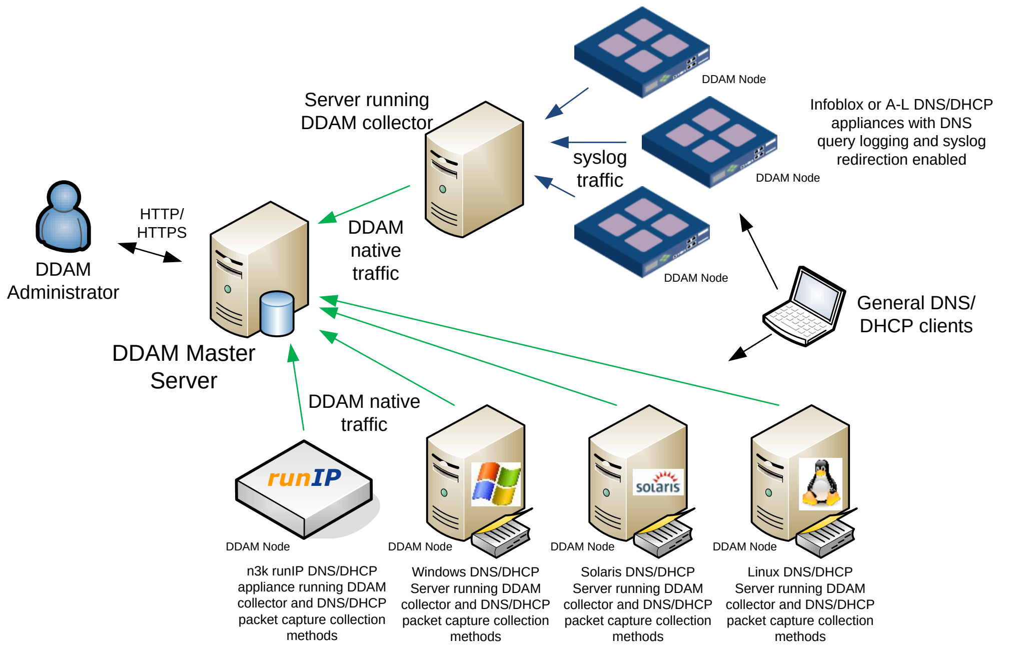
Collectors, or DDAM collectors, are where DNS and DHCP data is collected. Data can be collected in a number of ways to support various DNS and DHCP implementations. The way in which data is collected is referred to as a collection method.

Each collection method specifies whether DNS or DHCP traffic is to be collected, and whether the collection is performed via packet capture or syslog messages.

Each collection method is associated with a node. A node represents a DNS and/or DHCP Server in DDAM and can have multiple collection methods attached (for instance, if a node is generating both DNS and DHCP traffic it will need to have two collection methods associated with it at a minimum). A collector can collect data for one or more nodes, for instance it may be processing syslog messages from several different DNS/DHCP servers.

For example, if a number of appliance based DNS servers are utilizing the BIND 9 DNS server implementation, query logging can be enabled and redirected via syslog to a server where a DDAM Collector has been installed. Many syslog feeds can be handed by a single collector. Each server that is generating traffic is called a node.

The following diagram illustrates the relationship between the DDAM Master server, DDAM collectors and individual nodes:


DDAM Node
Server running DDAM collector
Infoblox or A-L DNS/DHCP appliances with DNS query logging and syslog redirection enabled
syslog traffic
DDAM Node
DDAM Administrator
HTTP/ HTTPS
DDAM native traffic
DDAM Node
General DNS/ DHCP clients
DDAM Master Server
DDAM native traffic
runIP
DDAM Node
DDAM Node
DDAM Node
DDAM Node
n3k runIP DNS/DHCP appliance running DDAM collector and DNS/DHCP packet capture collection methods
Windows DNS/DHCP Server running DDAM collector and DNS/DHCP packet capture collection methods
Solaris DNS/DHCP Server running DDAM collector and DNS/DHCP packet capture collection methods
Linux DNS/DHCP Server running DDAM collector and DNS/DHCP packet capture collection methods

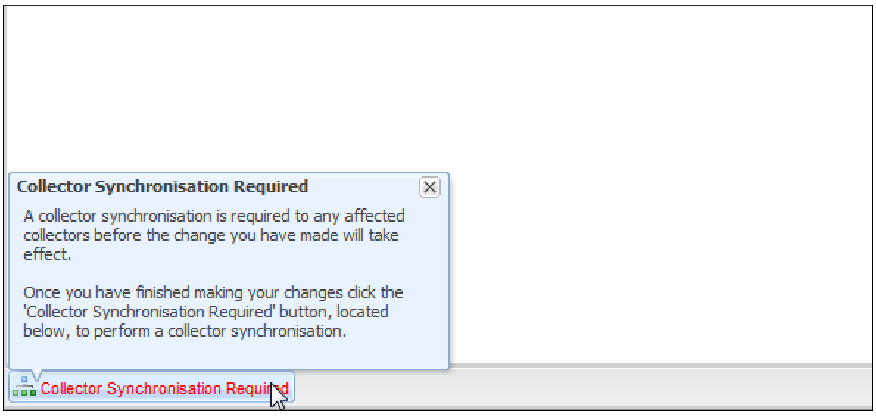
For more information on collectors and nodes, please refer to section 4.4.

1.3 Collector Synchronization

Some changes within the user interface require what is called a "Collector Synchronization" to take place.

This involves updating collectors with configuration information detailing how data should be collected, for what nodes, what alerts have been configured and how alerts are dispatched.

If a change is made that requires a collector synchronization, and the appropriate permissions have been granted, a blue pop-up alert will be displayed at the bottom left of the user interface directing the user to click the "Collector Synchronization Required" button:



Collector Synchronisation Required

A collector synchronisation is required to any affected collectors before the change you have made will take effect.

Once you have finished making your changes click the 'Collector Synchronisation Required' button, located below, to perform a collector synchronisation.

If other changes are pending that will also require a collector synchronization, it is advisable to make those changes before clicking the "Collector Synchronization Required" button.

Refer to the section 4.4.3 for more information on collector synchronization.

1.4 Product License

DDAM is licensed on a per node basis. The product license comes in the form of a text file with a number of license blocks, similar to the following:

```
generated_at: 1277750935
license_id: id
serial: 1
valid_from: -1
valid_to: 1277751000
signature: 51 7f 59 ba f2 6e 30 68 f1 49 8b ...

generated_at: 1277750935
license_id: id
serial: 2
valid_from: -1
valid_to: 1277751000
signature: 6c c7 e2 89 ff bb 4d 40 22 f1 6c ...
```

NOTE: Not all fields may be present, and other fields might exist.

If the product is licensed for 10 nodes, 10 blocks will exist with 10 different "serial" numbers. Within the product, licenses are assigned by associating a license serial number to a node. License serial numbers can be re-assigned within the product to different nodes.

If a server is both a DNS and DHCP server it is represented as a single node, and thus only one license serial number is required.

When a product license expires, data collection stops on all collectors. However, it will still be possible to view alert and report data.

Refer to section 4.1 for more information on applying product licenses.

Chapter

2

2 Installation & Upgrade

2.1 Bug Fixes & Enhancements

Please refer to the DDAM Release Notes for a list of bug fixes and enhancements that have been included in this release of DDAM.

2.2 Hardware Requirements

NOTE: For testing and evaluation, slower hardware can be utilized and much less disk space will typically be required.

The following hardware requirements are for DDAM Master Servers and DDAM Collector servers which will be utilized for syslog collection.

CPU	Intel Xeon X5560 2.80GHz processor or similar
Disk	Minimum 100GB 15k RPM SAS or similar
Memory	Minimum 4GB (8GB recommended)

2.3 System Requirements

Installation is supported on the following platforms:

- Solaris 8, 9 & 10
- Red Hat Enterprise Linux 3, 4 & 5
- Debian Linux 4, 5, 6
- Windows 2000, 2003 & 2008
- runIP 2.0, 2.1, 2.2 & 2.3

2.3.1 Windows 2000

If installing a collector for the purpose of syslog collection, Windows 2000 is not supported. Otherwise the collector can be installed on any of the above supported platforms. Windows 2000 doesn't support the functions required to calculate time zone information as part of the collection process.

2.3.2 Windows 2003

Installation on 32bit and 64bit Windows 2003 platforms require the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). This can be obtained from the following location:

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5638

2.4 Installation & Upgrade

Upgrades are performed by following the installation steps as detailed in the following sections.

2.4.1 Windows

NOTE: The User Access Control (UAC) feature available on some Windows operating systems (for example Windows 2008) prevents a required kernel driver service from being installed. This feature must be disabled during installation.

Double click the "ddam-x.x.x-windows.exe" Windows installer and follow the installation wizard.

2.4.2 Linux

Transfer the "ddam-x.x.x-linux.tgz" installation package into the "/tmp" directory on the server where it is to be installed.

Unpack and start the installation wizard using the following commands:

```
cd /tmp
```

```
gunzip ddam-x.x.x-linux.tgz

tar -xvf ddam-x.x.x-linux.tar

cd ddam-x.x.x-linux

./install
```

2.4.3 Solaris

Transfer the "ddam-x.x.x-linux.tgz" installation package into the "/tmp" directory on the server where it is to be installed.

Unpack and start the installation wizard using the following commands:

```
cd /tmp

gunzip ddam-x.x.x-linux.tgz

tar -xvf ddam-x.x.x-linux.tar

cd ddam-x.x.x-linux

./install
```

2.4.4 runIP

Upload the DDAM runIP package to the runIP management station.

As the DDAM runIP package is a configurable package, it must first be cloned. Under the "Manage Packages" menu, select the "ddam" package and click the "Create New Instance" button.

To configure the package, click the "edit version" link. After the package has been configured, click "Save" and "[Back]".

The package can then be deployed to the appropriate runIP appliances.

During package deployment appropriate iptables rules are added so that the DDAM master can connect to DDAM collectors, a so that syslog collection can occur.

2.5 Un-installation

The following sections detail the un-installation procedure that should be executed for each platform.

2.5.1 Windows

Un-installation is performed by executing the "uninstall.exe" un-installer found under the installation directory.

2.5.2 Linux

Stop the DDAM daemons using the following command:

```
<installation-directory>/ctl stop
```

The installation directory can be deleted using the rm –rf <installation-directory> command.

NOTE: Any links created to the above start script will also need to be removed.

2.5.3 Solaris

Stop the DDAM daemons using the following command:

```
<installation-directory>/ctl stop
```

The installation directory can be deleted using the rm –rf <installation-directory> command.

NOTE: Any links created to the above start script will also need to be removed.

2.5.4 runIP

Un-installation is performed by removing the DDAM runIP package from the appliance.

Chapter

3

3 User Interface

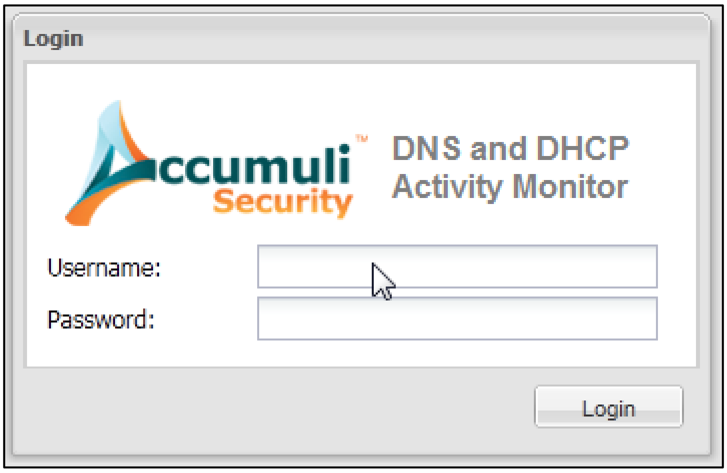
3.1 Accessing the User Interface

After installing the DDAM Master Server, the web interface can be accessed via the following URL:

`https://<master>:<port>`

Where <master> is the IP address or hostname of the DDAM Master Server and <port> is the TCP port specified during installation (this can be found in the "port" option configured in the <installation>/http-serverd.conf file on the master).

Once connected, a login dialog box will be displayed. Upon first installation a default "admin" user will exist. By default the admin users password is "admin", this should be changed immediately.

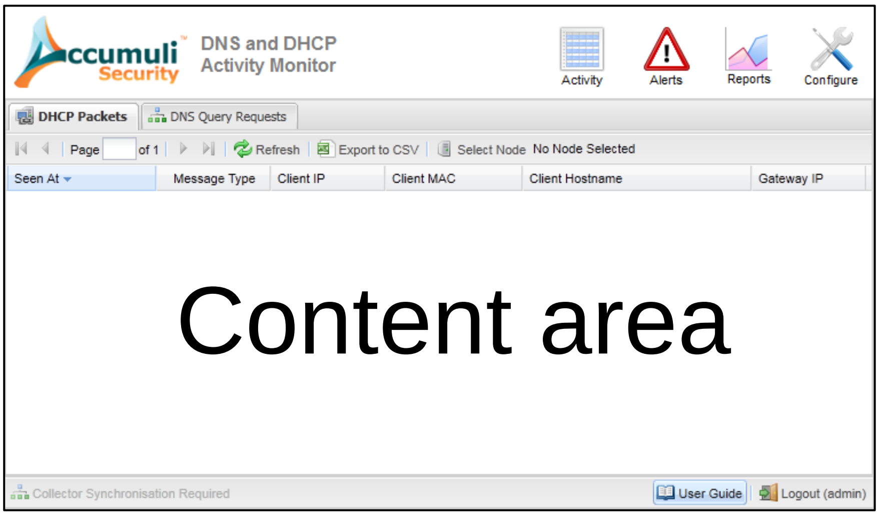


3.2 Time zone

All dates and times displayed in the user interface use the time zone of the DDAM Master Server.

3.3 Layout & Navigation

Once logged into the user interface the DDAM user interface will be displayed and the administrator will be asked to select a node. Either select a node or simply hit "Cancel" at this stage (information on adding nodes can be found in section 4.4).



At the top right of the page are icons that are used to access the main features of the product (Activity, Alerts, Reports and Configure). If the appropriate privileges have not been granted, access to these features may not be available (and the corresponding icon will not be displayed).

The area below the icons is referred to as the content area. Upon clicking an icon at the top of the interface the content area will change.

At the top of the content area are tabs. These tabs are used to access the sub-features of a particular feature. Upon clicking one of these tabs the content area will again change.

Below the tabs is a toolbar. The contents of this toolbar will depend on which icon and tab have been selected.

At the bottom of the page is another toolbar. On the left of this toolbar is the "Collector Synchronization Required" button. If a change is made that requires a collector synchronization, and the appropriate privileges have been granted, this button will become enabled and a blue pop-up displayed above it to indicate that one is required.

To the right of this toolbar is the "User Guide" button used to access the installation and user guide, and the "Logout" button used to logout of the user interface.

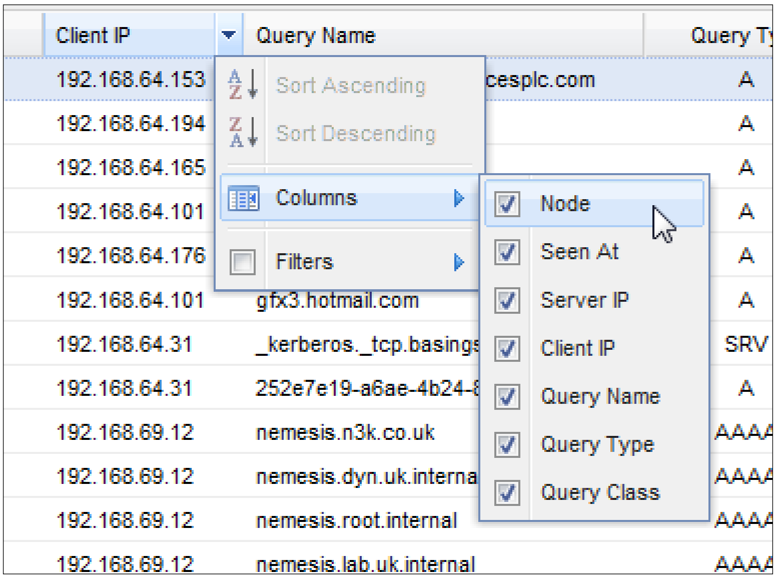
3.3.1 Right Click Menus

When configuring various items in the user interface, right click menus are typically employed to perform actions on a specific item. Not all areas within the GUI employ right click menus as they are only deployed where necessary. This manual will detail areas within the user interface where right click menus are available.

3.3.2 Grid Column Selection & Ordering

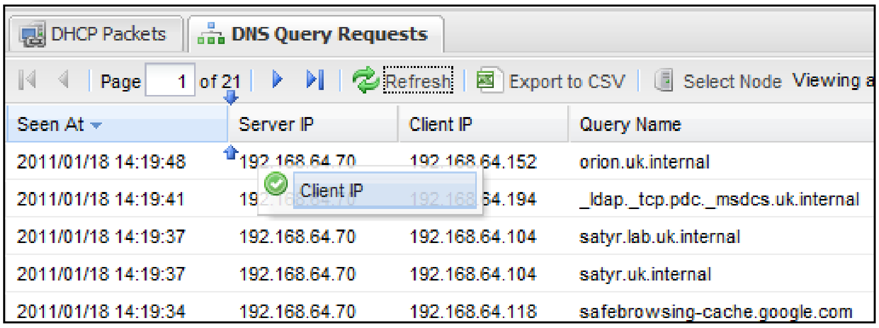
Various tabs throughout the user interface employ grids to allow tabular data to be viewed, and in cases, sorted and filtered.

The various columns which are displayed in a grid can be enabled or disabled by hovering over one of the column headers and clicking the down facing arrow that appears, then selecting the "Columns" sub-menu and ticking/unticking columns that are required or not required:



When exporting data, only the columns which are displayed will be exported.

The order of columns can also be changed by clicking on the column heading and moving it to the desired location:



Seen At	Server IP	Client IP	Query Name
2011/01/18 14:19:48	192.168.64.70	192.168.64.152	orion.uk.internal
2011/01/18 14:19:41	19	64.194	_ldap._tcp.pdc._msdcs.uk.internal
2011/01/18 14:19:37	192.168.64.70	192.168.64.104	satyr.lab.uk.internal
2011/01/18 14:19:37	192.168.64.70	192.168.64.104	satyr.uk.internal
2011/01/18 14:19:34	192.168.64.70	192.168.64.118	safebrowsing-cache.google.com

NOTE: *Customization of columns is not persistent across logins. If the user logs out and logs in, the columns will be reset back to the default layout.*

When exporting data, the columns will be exported in the order they are being displayed.

Most grids provide some sort of sorting functionality, this is achieved by clicking the heading of the column that needs to be sorted or by using the same pop-up menu as above, and choosing between the "Sort Ascending" and "Sort Descending" options (if sorting is disabled for the selected column, these two options will be disabled).

3.3.3 Grid Filters

Various grids throughout the user interface offer a filtering mechanism. The type of filtering available will depend on the data for which the column represents.

Throughout this document where filtering is supported, a section will define the filter types for each grid column. The filter types and their supported filter formats are defined as follows:

Date/Time

In all of the following cases, DATE is in the format of "YYYY/MM/DD hh:mm:ss", where "YYYY", "MM" and "DD" are a year, month and day respectively, and "hh:mm:ss" are hour, minute and second respectively. For example "2010/09/10 10:59:00" represents the 10th of September 2010 at 10:59:00.

It is possible to exclude certain parts of the date from the right, so for example "2010/09/10 will filter records between "2010/09/10 00:00:00" and "2010/09/10 23:59:00", and "2010/09/10 15:00" will filter records between "2010/09/10 15:00:00" and "2010/09/10 15:00:59".

Format	Description
>DATE	Filter for records older than this date, for example ">2010/09/01".
<DATE	Filter for records newer than this date, for example "<2010/09/01".
DATE	Filter for records at this time, for example "2010/09/01" or "2010/09/01 15".

String

String filters can be prefixed with "!" to negate the filter (e.g. "!*.uk.internal")

Format	Description

STRING	Filter for records that match this string exactly.
*STRING	Filter for records that end with this string.
STRING*	Filter for records that begin with this string.
STRING	Filter for records that contain this string.

IP Address

IP Address filters can be prefixed with "!" to negate the filter (e.g. "!10/8")

Format	Description
x.x	Filter for records that have this prefix, for example "10" or "192.168.64".
x.x/m	Filter for records on this subnet, for example "10/24" or "192.168.64/24".
x.x.x.x	Filter for records matching this IP address, for example "192.168.64.181".

Number

Format	Description
NUMBER	Filter for records that match this number exactly, for example "10".
!NUMBER	Filter for records that do NOT match this number exactly, for example "!10".
>NUMBER	Filter for records that are more than this number, for example ">9".
<NUMBER	Filter for records that are less than this number,

	for example "<10".

Enum

This type of filter allows a space separated list of values to be entered. The values can be a string or a numerical value and are used where a string normally has a numerical representation within the DNS or DHCP protocol. For instance, a DHCP INFORM packet is actually DHCP message type 8, so a filter can be defined that either uses the string "INFORM" or the numerical code "8". Similarly, a DNS "A" record has a numerical type code of "1", so a DNS record type filter could use "A" or "1".

The reason this filter accepts either strings or numerical values is that as new DNS or DHCP protocol developments are incorporated, the string representation of the numerical value may not have been defined yet. For instance, several years ago a new DNS record type of "SPF" was proposed with a numerical type code of "99". For several years, many products including BIND itself did not support the string representation of "SPF" but were able to use the numerical type code "99" with no modification. Filters based on enum fields are thus able to support new developments using the numerical representation (usually defined in an RFC).

Enum filters can be prefixed with "!" to negate the filter (e.g. "! a ptr") ")

The text and numerical representation of various DNS and DHCP parameters are listed within Appendices A, B and C.

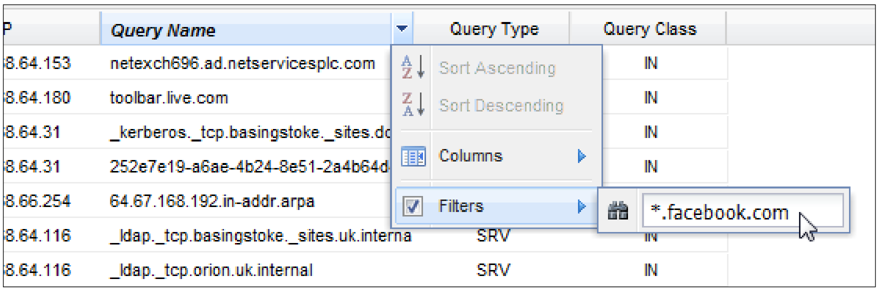
Example filters

NOTE: *When disabling a filter, it is necessary to click "Refresh" to ensure that the grid is reset.*

The following examples demonstrate how filters can be used. When a filter has been applied, the column heading will change to ***emboldened italics***. To disable a filter, simply uncheck the box next to the word "Filters" on the column menu.

Multiple filters can be defined simultaneously. The ***emboldened italics*** within the column headings will indicate which columns have filters defined.

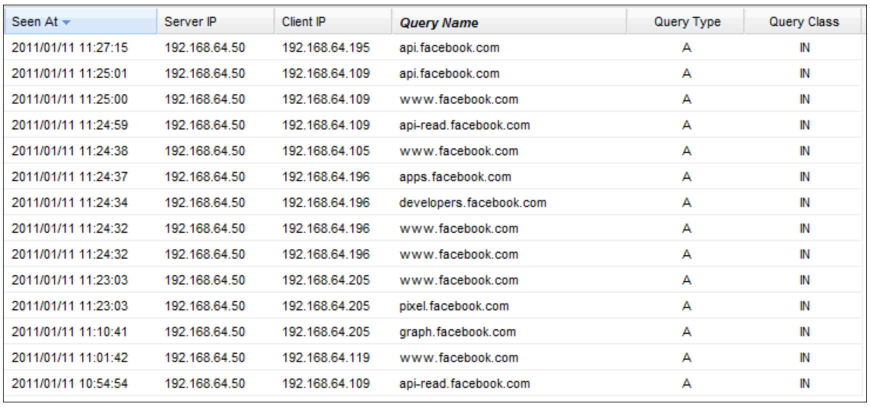
In this first example, the DNS activity log is being filtered using a wildcard "*" for queries that end with facebook.com:



*.facebook.com

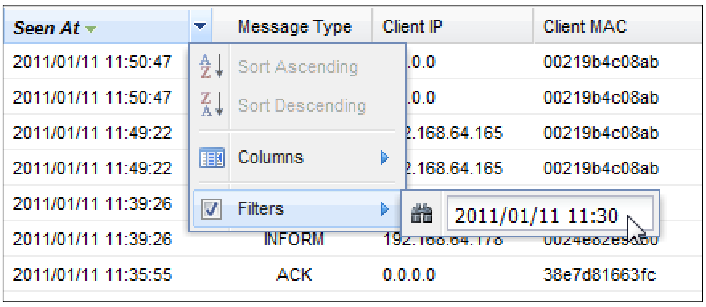
P	Query Name	Query Type	Query Class
8.64.153	netexch696.ad.netservicesplc.com		IN
8.64.180	toolbar.live.com		IN
8.64.31	_kerberos._tcp.basingstoke._sites.dc		IN
8.64.31	252e7e19-a6ae-4b24-8e51-2a4b64d		IN
8.66.254	64.67.168.192.in-addr.arpa		
8.64.116	_ldap._tcp.basingstoke._sites.uk.interna	SRV	[illegible]
8.64.116	_ldap._tcp.orion.uk.internal	SRV	IN

The resultant display only lists DNS queries that match the filter:



Seen At	Server IP	Client IP	Query Name	Query Type	Query Class
2011/01/11 11:27:15	192.168.64.50	192.168.64.195	api.facebook.com	A	IN
2011/01/11 11:25:01	192.168.64.50	192.168.64.109	api.facebook.com	A	IN
2011/01/11 11:25:00	192.168.64.50	192.168.64.109	www.facebook.com	A	IN
2011/01/11 11:24:59	192.168.64.50	192.168.64.109	api-read.facebook.com	A	IN
2011/01/11 11:24:38	192.168.64.50	192.168.64.105	www.facebook.com	A	IN
2011/01/11 11:24:37	192.168.64.50	192.168.64.196	apps.facebook.com	A	IN
2011/01/11 11:24:34	192.168.64.50	192.168.64.196	developers.facebook.com	A	IN
2011/01/11 11:24:32	192.168.64.50	192.168.64.196	www.facebook.com	A	IN
2011/01/11 11:24:32	192.168.64.50	192.168.64.196	www.facebook.com	A	IN
2011/01/11 11:23:03	192.168.64.50	192.168.64.205	www.facebook.com	A	IN
2011/01/11 11:23:03	192.168.64.50	192.168.64.205	pixel.facebook.com	A	IN
2011/01/11 11:10:41	192.168.64.50	192.168.64.205	graph.facebook.com	A	IN
2011/01/11 11:01:42	192.168.64.50	192.168.64.119	www.facebook.com	A	IN
2011/01/11 10:54:54	192.168.64.50	192.168.64.109	api-read.facebook.com	A	IN

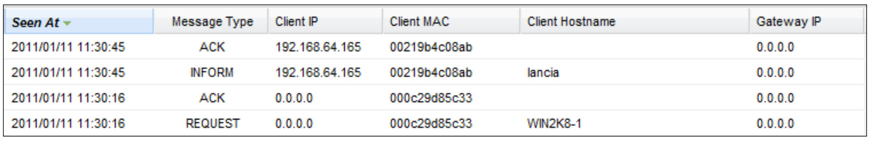
In this example, DHCP activity is being filtered for a specific date and time:



2011/01/11 11:30

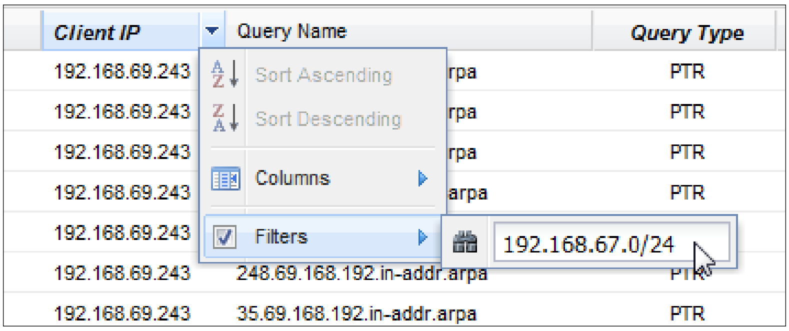
Seen At	Message Type	Client IP	Client MAC
2011/01/11 11:50:47		.0.0	00219b4c08ab
2011/01/11 11:50:47		.0.0	00219b4c08ab
2011/01/11 11:49:22		2.168.64.165	00219b4c08ab
2011/01/11 11:49:22		2.168.64.165	00219b4c08ab
2011/01/11 11:39:26			
2011/01/11 11:39:26	INFORM	[illegible]	[illegible]
2011/01/11 11:35:55	ACK	0.0.0.0	38e7d81663fc

The resultant display only lists DHCP messages that match the filter:



Seen At	Message Type	Client IP	Client MAC	Client Hostname	Gateway IP
2011/01/11 11:30:45	ACK	192.168.64.165	00219b4c08ab		0.0.0.0
2011/01/11 11:30:45	INFORM	192.168.64.165	00219b4c08ab	lancia	0.0.0.0
2011/01/11 11:30:16	ACK	0.0.0.0	000c29d85c33		0.0.0.0
2011/01/11 11:30:16	REQUEST	0.0.0.0	000c29d85c33	WIN2K8-1	0.0.0.0

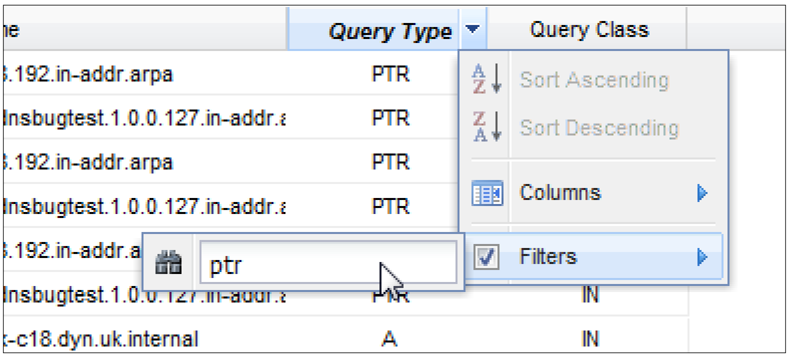
In this example, DNS activity is being filtered on both the Client IP address and Query Type. The Client IP address filter will only reveal DNS queries from a particular address range:



Client IP	Query Name	Query Type
192.168.69.243	rpa	PTR
192.168.69.243	rpa	PTR
192.168.69.243	rpa	PTR
192.168.69.243	arpa	PTR
192.168.69.243		
192.168.69.243	248.69.168.192.in-addr.arpa	PTR
192.168.69.243	35.69.168.192.in-addr.arpa	PTR

192.168.67.0/24

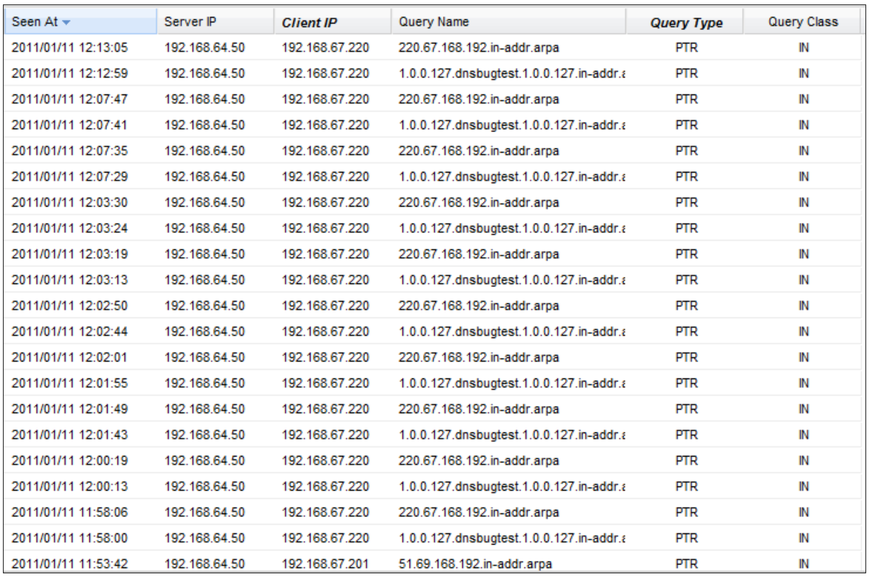
The Query Type filter will only reveal PTR type DNS queries:



ne	Query Type	Query Class
.192.in-addr.arpa	PTR	
lnsbugtest.1.0.0.127.in-addr.ε	PTR	
.192.in-addr.arpa	PTR	
lnsbugtest.1.0.0.127.in-addr.ε	PTR	
.192.in-addr.a		
lnsbugtest.1.0	PTR	IN
-c18.dyn.uk.internal	A	IN

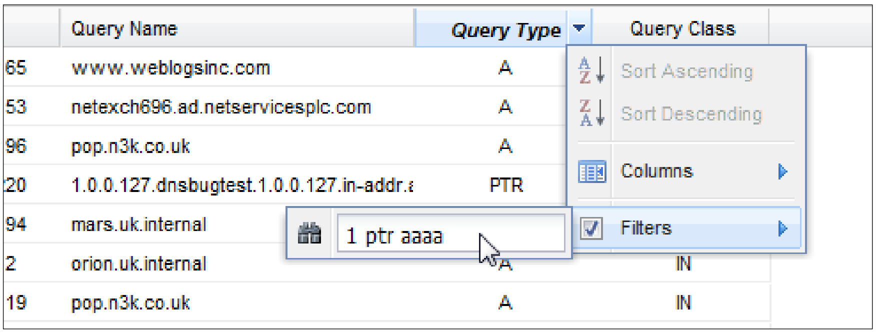
ptr

The resultant output lists all DNS queries from the network 192.168.67.0/24 with a query type of PTR:



Seen At	Server IP	Client IP	Query Name	Query Type	Query Class
2011/01/11 12:13:05	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:12:59	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:07:47	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:07:41	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:07:35	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:07:29	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:03:30	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:03:24	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:03:19	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:03:13	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:02:50	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:02:44	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:02:01	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:01:55	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:01:49	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:01:43	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 12:00:19	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 12:00:13	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 11:58:06	192.168.64.50	192.168.67.220	220.67.168.192.in-addr.arpa	PTR	IN
2011/01/11 11:58:00	192.168.64.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	IN
2011/01/11 11:53:42	192.168.64.50	192.168.67.201	51.69.168.192.in-addr.arpa	PTR	IN

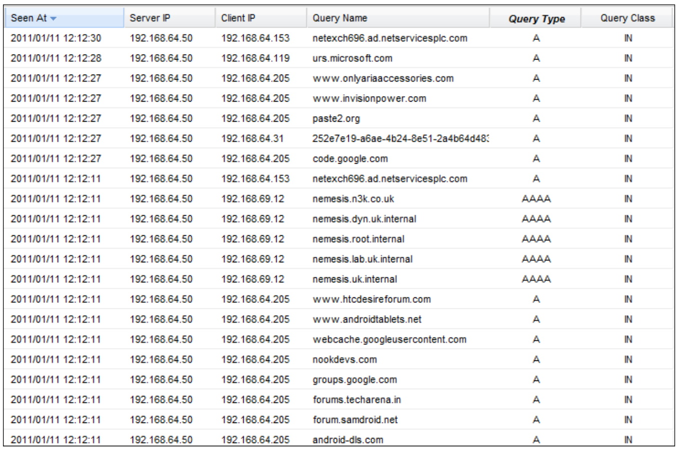
In this example, a DNS activity filter is used to filter records with a DNS Query Type of A, PTR and AAAA, note however that the number 1 is used to specify type A. Any DNS Query Type Code can be used in place of a DNS Query Type string. See Appendices A, B and C for lists of numerical codes that can be used.



	Query Name	Query Type	Query Class
65	www.weblogsinc.com	A	
53	netexch696.ad.netservicesplc.com	A	
96	pop.n3k.co.uk	A	
20	1.0.0.127.dnsbugtest.1.0.0.127.in-addr.a	PTR	
94	mars.uk.internal		
2	orion.uk.internal	A	IN
19	pop.n3k.co.uk	A	IN

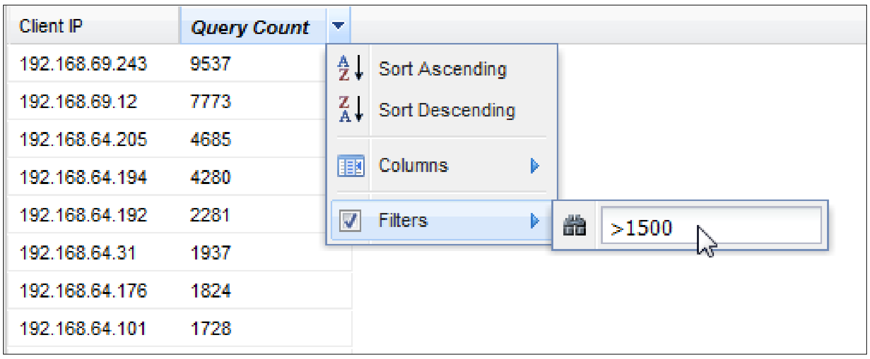
1 ptr aaaa

The resultant output lists DNS queries that match the specified filter:



Seen At	Server IP	Client IP	Query Name	***Query Type***	Query Class
2011/01/11 12:12:30	192.168.64.50	192.168.64.153	netexch696.ad.netservicesplc.com	A	IN
2011/01/11 12:12:28	192.168.64.50	192.168.64.119	urs.microsoft.com	A	IN
2011/01/11 12:12:27	192.168.64.50	192.168.64.205	www.onlyariaaccessories.com	A	IN
2011/01/11 12:12:27	192.168.64.50	192.168.64.205	www.invisionpower.com	A	IN
2011/01/11 12:12:27	192.168.64.50	192.168.64.205	paste2.org	A	IN
2011/01/11 12:12:27	192.168.64.50	192.168.64.31	252e7e19-a6ae-4b24-8e51-2a4b64d48	A	IN
2011/01/11 12:12:27	192.168.64.50	192.168.64.205	code.google.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.153	netexch696.ad.netservicesplc.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.69.12	nemesis.n3k.co.uk	AAAA	IN
2011/01/11 12:12:11	192.168.64.50	192.168.69.12	nemesis.dyn.uk.internal	AAAA	IN
2011/01/11 12:12:11	192.168.64.50	192.168.69.12	nemesis.root.internal	AAAA	IN
2011/01/11 12:12:11	192.168.64.50	192.168.69.12	nemesis.lab.uk.internal	AAAA	IN
2011/01/11 12:12:11	192.168.64.50	192.168.69.12	nemesis.uk.internal	AAAA	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	www.htcdesireforum.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	www.androidtablets.net	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	webcache.googleusercontent.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	nookdevs.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	groups.google.com	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	forums.techarena.in	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	forum.samdroid.net	A	IN
2011/01/11 12:12:11	192.168.64.50	192.168.64.205	android-dls.com	A	IN

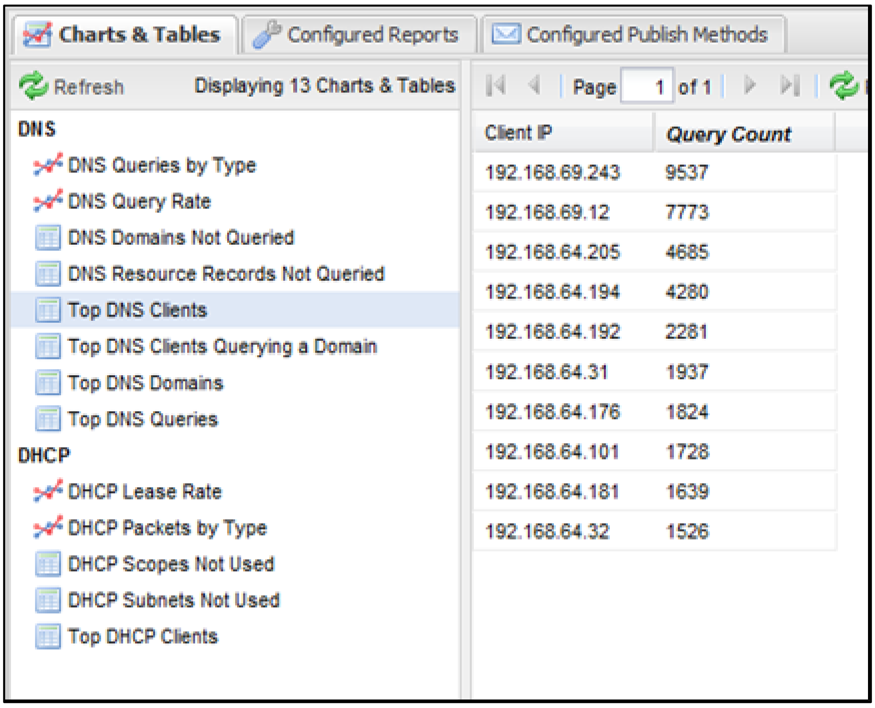
In this example, the "Top DNS Clients" report is being filtered to only show clients with more than 1500 queries registered. This could be useful in order to prevent many pages of data being generated:



Client IP	***Query Count***
192.168.69.243	9537
192.168.69.12	7773
192.168.64.205	4685
192.168.64.194	4280
192.168.64.192	2281
192.168.64.31	1937
192.168.64.176	1824
192.168.64.101	1728

☑ Filters: >1500

The resultant report now does not list any clients with fewer than 1500 queries:



Client IP	*Query Count*
192.168.69.243	9537
192.168.69.12	7773
192.168.64.205	4685
192.168.64.194	4280
192.168.64.192	2281
192.168.64.31	1937
192.168.64.176	1824
192.168.64.101	1728
192.168.64.181	1639
192.168.64.32	1526

3.3.4 Grid Export

Various grids throughout the user interface offer the ability to export data via an "Export to CSV" button. Data is exported in CSV format and the selected columns, sorting, and filters are adhered to.

Chapter
4

4 Configuration

Configuration of DDAM is performed via the Configure icon:

Configure

NOTE: If the appropriate administrative rights have not been granted, this icon may not be displayed.

The following sections provide detail on each tab available once the Configure icon has been selected.

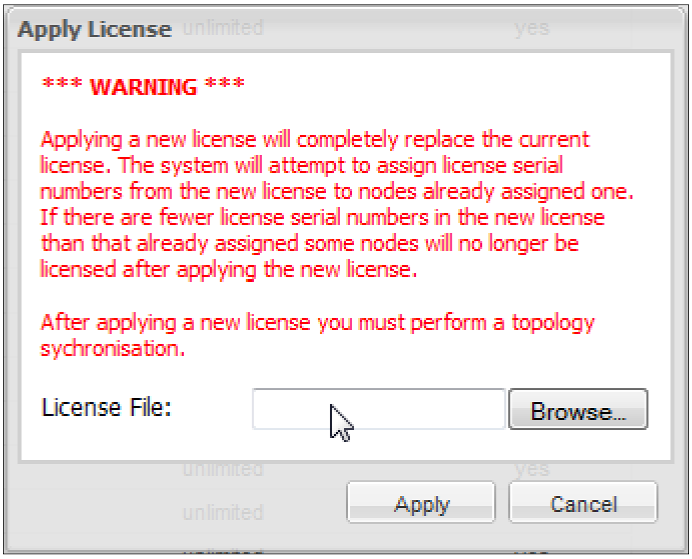
4.1 Product License

Before DDAM will collect any data, a product license must be applied. A product license can be obtained from the vendor that DDAM was purchased from. The product license specifies how many nodes can be enabled for data collection.

The product license contains a number of license serial numbers – each serial number will be assigned to a node, therefore it is important to ensure that the license contains enough serial numbers to activate all the nodes that data collection should be enabled for.

Once a product license has been obtained, it can be uploaded from the "Product License" tab by clicking the "Apply License" button.

After specifying the location of the license file, click the Apply button and the product license will be applied.



Apply License

***** WARNING *****

Applying a new license will completely replace the current license. The system will attempt to assign license serial numbers from the new license to nodes already assigned one. If there are fewer license serial numbers in the new license than that already assigned some nodes will no longer be licensed after applying the new license.

After applying a new license you must perform a topology sychronisation.

License File:

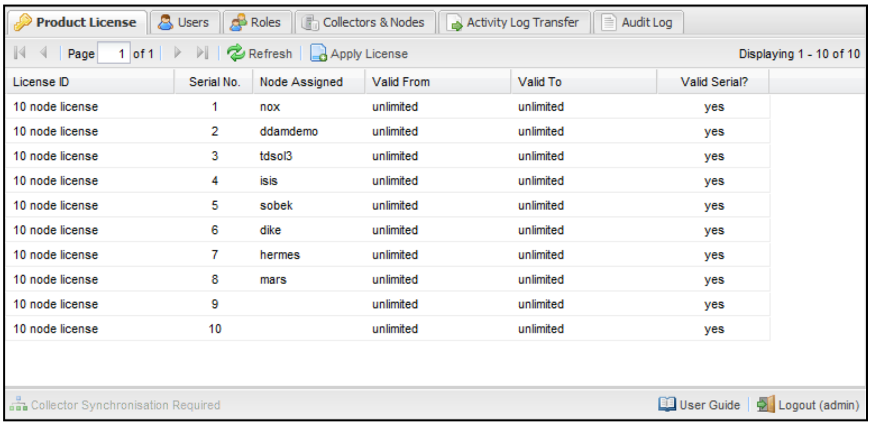
NOTE: *A Collector Synchronization is required after making any changes to the product license.*

If a number of nodes have already been defined in the system and have license serial numbers associated with them, the system will try to maintain these associations so long as there enough license serial numbers in the new product license.

Under the Product License tab an entry for each license serial number is displayed with the following columns:

Column	Description
License ID	License ID found in the product license. This enables an administrator to detect which license is currently applied.
Serial No.	The license serial number which can be assigned or unassigned.
Node Assigned	If this license serial is assigned to a node, this column displays the name of the node.
Valid From	Date from which the license serial is valid from. This column will display "unlimited" if the license has no valid from date.
Valid To	Date to which the license serial is valid. This column will display "unlimited" if the license has

	no valid to date.
Valid Serial?	This column will display either "yes" if the license serial is valid, or "no" if it is not.



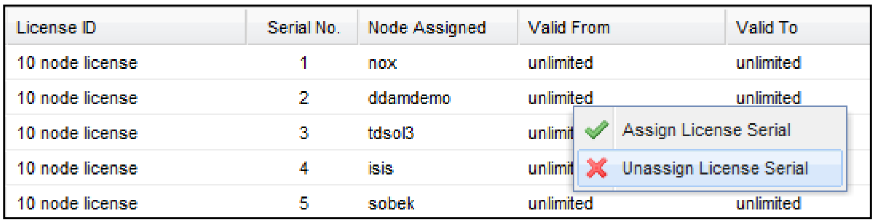
License ID	Serial No.	Node Assigned	Valid From	Valid To	Valid Serial?
10 node license	1	nox	unlimited	unlimited	yes
10 node license	2	ddamdemo	unlimited	unlimited	yes
10 node license	3	tdsol3	unlimited	unlimited	yes
10 node license	4	isis	unlimited	unlimited	yes
10 node license	5	sobek	unlimited	unlimited	yes
10 node license	6	dike	unlimited	unlimited	yes
10 node license	7	hermes	unlimited	unlimited	yes
10 node license	8	mars	unlimited	unlimited	yes
10 node license	9		unlimited	unlimited	yes
10 node license	10		unlimited	unlimited	yes

Collector Synchronisation Required

If a node is deleted, its associated license serial number will become free, allowing this serial number to be re-assigned to another node.

After uploading a license, each serial number can be assigned by right clicking the license serial and choosing "Assign License Serial". Likewise a license serial can be un-assigned by right-clicking the license serial and choosing "Unassign License Serial".

__NOTE:__ A Collector Synchronization is required after making any changes to license serial number associations.

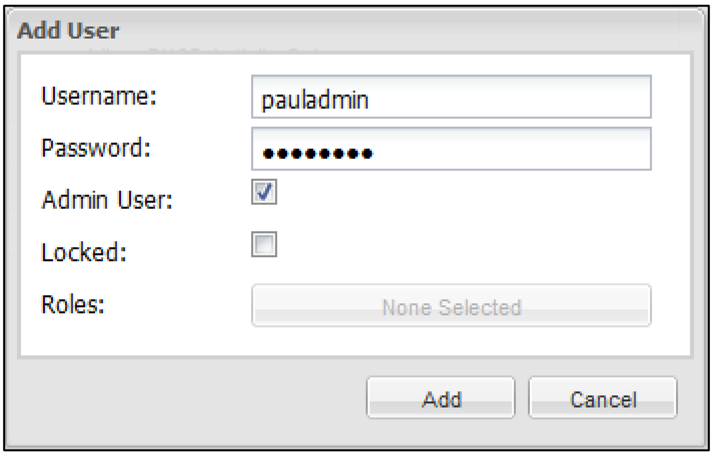


License ID	Serial No.	Node Assigned	Valid From	Valid To
10 node license	1	nox	unlimited	unlimited
10 node license	2	ddamdemo	unlimited	unlimited
10 node license	3	tdsol3	unlimit	
10 node license	4	isis	unlimit	
10 node license	5	sobek	unlimited	unlimited

Refer to section 1.4 for more information on the product license.

4.2 Users

Two types of user can be configured in DDAM, either an administrative user or standard user. The type of user is selected upon user addition or modification by checking the "Admin User" checkbox.



Add User

Username: pauladmin

Password: •••••••••

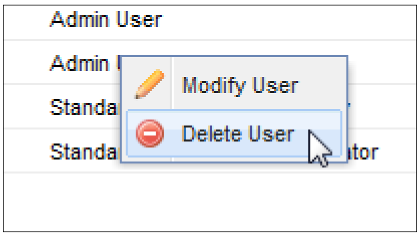
Admin User: ☑

Locked: ☐

Roles: None Selected

Admin users have full access to the product and its configuration. Standard users only have access to areas of the product specified within roles that are assigned to them.

Users can be added by clicking the "Add User" button, or modified/deleted by using the right click menu.



The following fields can be configured when adding and modifying a user:

NOTE: *In the case of the user called "admin", only the password field can be modified, the user itself cannot be deleted.*

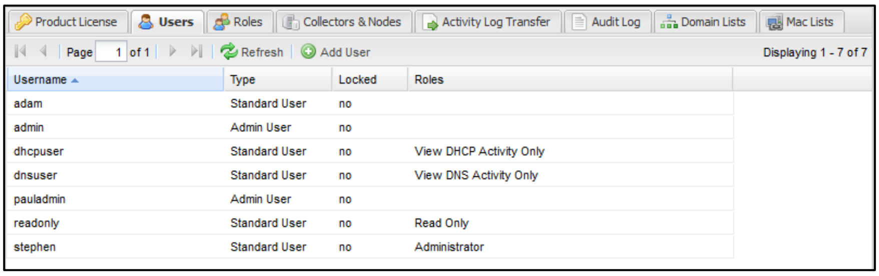
Field	Description
Username	The name which the user will use to login to DDAM.
Password	Password for the user. There is no restriction on this field.
Admin User	This box should be checked if this user is to be an admin user. The Role selection button will be disabled if this is checked.
Locked	This box should be checked if the user account is to be disabled. The user will not be permitted to login to the user interface.
Roles	Click this button to select which Roles should be assigned to the user. This option is only available to standard users (i.e. "Admin User" box is left unchecked).

NOTE: If all admin users have been accidently locked the “unlock-user” utility can be used to un-lock a user. Refer to section 9.6 for more information on this utility.

Under the Users tab, an entry for each user defined is displayed with the following columns:

Column	Description
Username	The name which the user will use to login to DDAM.
Type	Whether this user is defined as an admin user or not. Standard User" will be displayed for non-

	admin users.
Locked	Whether this user account is disabled.
Roles	A list of roles which have been assigned to the user.

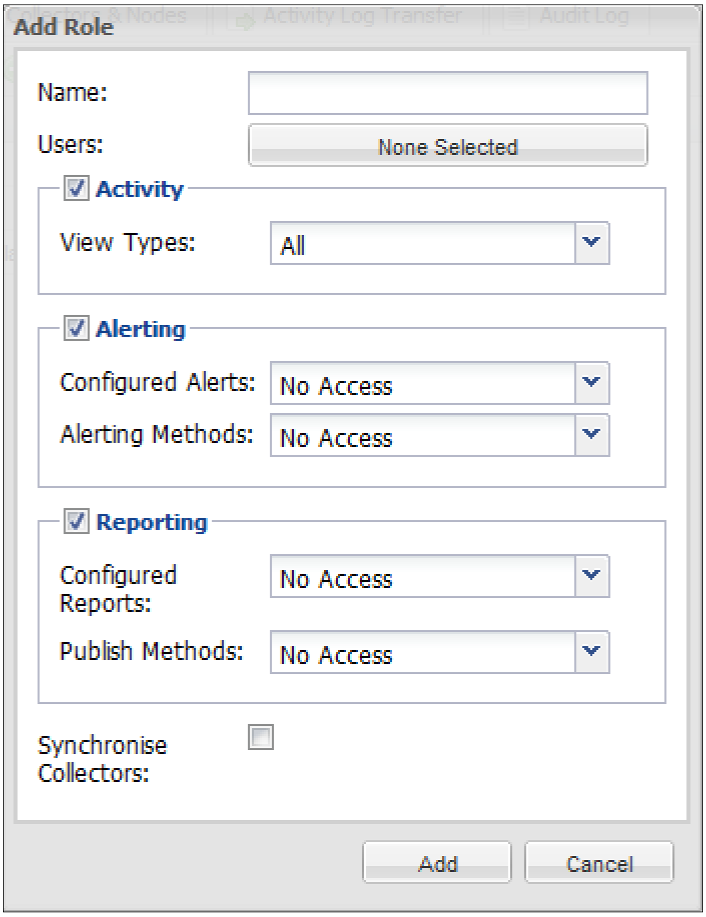


Username	Type	Locked	Roles
adam	Standard User	no	
admin	Admin User	no	
dhcpuser	Standard User	no	View DHCP Activity Only
dnsuser	Standard User	no	View DNS Activity Only
pauladmin	Admin User	no	
readonly	Standard User	no	Read Only
stephen	Standard User	no	Administrator

4.3 Roles

Access to DDAM for standard users is controlled using a role mechanism. This is accessed via the "Roles" tab. Each user may be assigned many roles. During a capability check to see if a user can perform an action, each role is consulted, and the user is allowed to perform the action if at least one role permits it.

Roles can be added by clicking the Add Role button, or modified/deleted by using the right click menu.



Add Role

Name:

Users: None Selected

☑ **Activity**

View Types: All

☑ **Alerting**

Configured Alerts: No Access

Alerting Methods: No Access

☑ **Reporting**

Configured Reports: No Access

Publish Methods: No Access

Synchronise Collectors: ☐

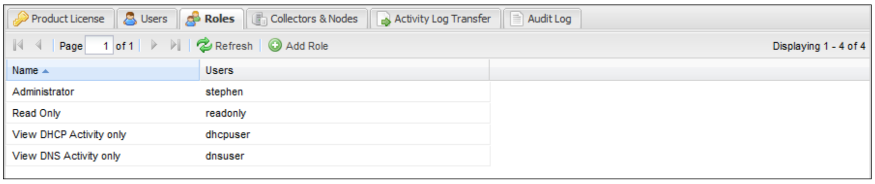
The following fields can be configured when adding and modifying a role:

Field	Description
Name	Name to assign the role.
Users	Click this button to select which users should be assigned the role.
Activity	Check this box if users assigned this role should be able to view activity under the Activity page.

Activity->View Types	Select which activity types users assigned this role should be able to view.
Alerting	Check this box if users assigned this role should be able to view the alert log under the Alert page.
Alerting->Configured Alerts	Select what access users assigned this role should have to Configured Alerts.
Alerting->Alerting Methods	Select what access users assigned this role should have to Configured Alerting Methods.
Reporting	Check this box if users assigned this role should be able to view charts and tables under the Report page.
Reporting->Configured Reports	Select what access users assigned this role should have to Configured Reports.
Reporting->Publish Methods	Select what access users assigned this role should have to configured Publish Methods.
Reporting->Synchronize Collectors	Check this box if users assigned this role should be able to perform collector Synchronizations when required.

Under the Roles tab an entry for each role defined is displayed with the following columns:

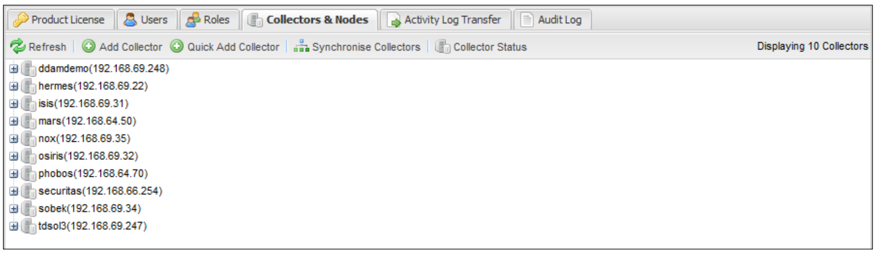
Column	Description
Name	The role name.
Users	A list of users which have been assigned the role.



Name	Users
Administrator	stephen
Read Only	readonly
View DHCP Activity only	dhcpuser
View DNS Activity only	dnsuser

4.4 Collectors & Nodes

The "Collectors & Nodes" tab enables an administrator to manage all the collectors and nodes defined in the system. This tab determines which systems perform data collection, which protocol they perform collection for, and how the collection is performed.



ddamdemo(192.168.69.248)
hermes(192.168.69.22)
isis(192.168.69.31)
mars(192.168.64.50)
nox(192.168.69.35)
osiris(192.168.69.32)
phobos(192.168.64.70)
securitas(192.168.66.254)
sobek(192.168.69.34)
tdsol3(192.168.69.247)

4.4.1 Introduction

A collector represents an entity on the network that has the DDAM collector agent installed. The collector agent can be installed on the central DDAM master server and/or remote servers spread around the network.

A collector agent can perform several tasks as follows:

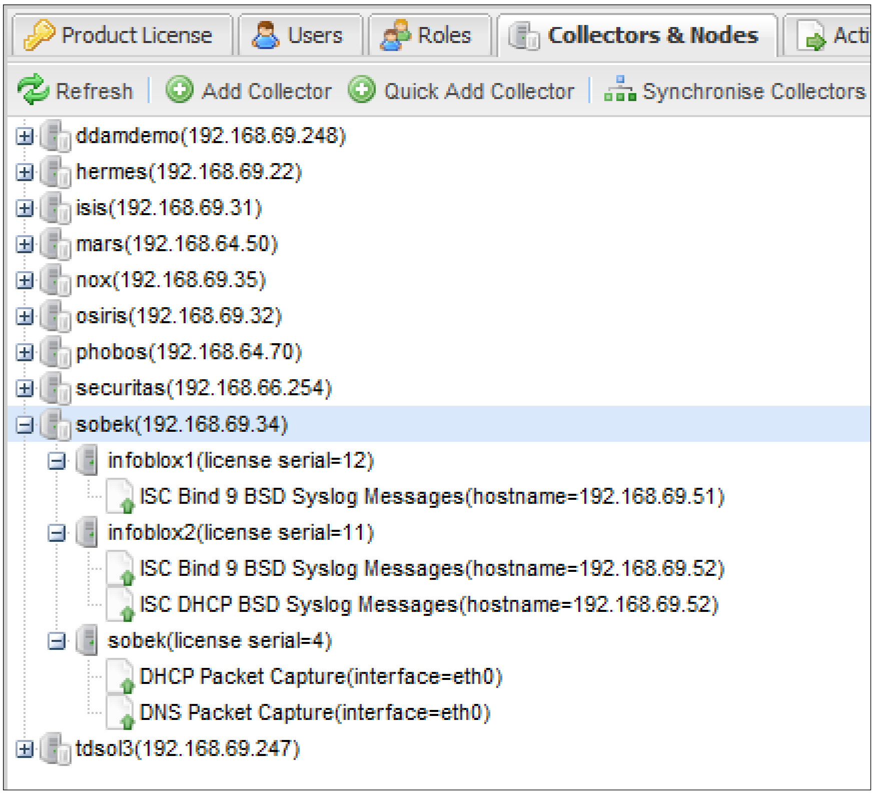
- Perform real-time raw DNS packet capture
- Perform real-time raw DHCP packet capture
- Receive and process syslog traffic containing ISC BIND querylog data
- Receive and process syslog traffic containing ISC DHCP log traffic
- Generate real-time alerts based on pre-configured alert definitions

Attached to each collector definition are nodes. Each node requires a license serial number to be assigned in order for that node to perform collection. Each node has one or more collection methods attached. A collection method consists of either a DNS or DHCP packet capture processor or an ISC BIND/DHCP syslog processor.

For real-time raw DNS and DHCP packet capture, each collector would normally have a node attached that is configured with either a DNS Packet Capture collection method, a DHCP Packet Capture collection method, or both collection methods.

However, a collector can also receive and process syslog traffic from devices where it is not possible to install a collector (e.g. Infoblox appliance). In these cases, additional nodes may be attached to an existing collector that has a syslog collection method attached. Therefore it is possible that a single collector could have several/many nodes attached; all performing syslog collection for different devices.

Collectors can be expanded within the "Collectors & Nodes" tab in order to view any attached nodes and collection methods.



- ddamdemo(192.168.69.248)
- hermes(192.168.69.22)
- isis(192.168.69.31)
- mars(192.168.64.50)
- nox(192.168.69.35)
- osiris(192.168.69.32)
- phobos(192.168.64.70)
- securitas(192.168.66.254)
- sobek(192.168.69.34)
  - infoblox1(license serial=12)
    - ISC Bind 9 BSD Syslog Messages(hostname=192.168.69.51)
  - infoblox2(license serial=11)
    - ISC Bind 9 BSD Syslog Messages(hostname=192.168.69.52)
    - ISC DHCP BSD Syslog Messages(hostname=192.168.69.52)
  - sobek(license serial=4)
    - DHCP Packet Capture(interface=eth0)
    - DNS Packet Capture(interface=eth0)
- tdsol3(192.168.69.247)

4.4.2 Configure

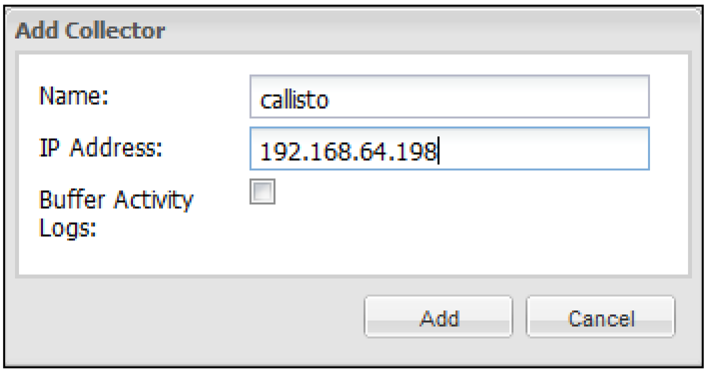
The first step in the configuration process involves defining a collector. Once a collector has been defined, a node, or multiple nodes can be added, finally the individual collection methods can be added to each of the nodes.

There are two mechanisms that can be used to define a new collector:

- "Add Collector" button
  - The "Add Collector" button enables collectors, nodes and collection methods all to be assigned and configured manually. This button has to be used if collection via syslog is required and a collector has not already been defined for this purpose.
- "Quick Add Collector" button

- The "Quick Add Collector" button will automatically define a collector, node, and DNS and DHCP packet capture collection methods in one easy step. The configuration can be modified afterwards if it does not meet the exact requirements e.g. DHCP Packet Capture collection method could be deleted.

If the "Add Collector" button is selected, a dialogue box asks for the name and IP address of the collector.



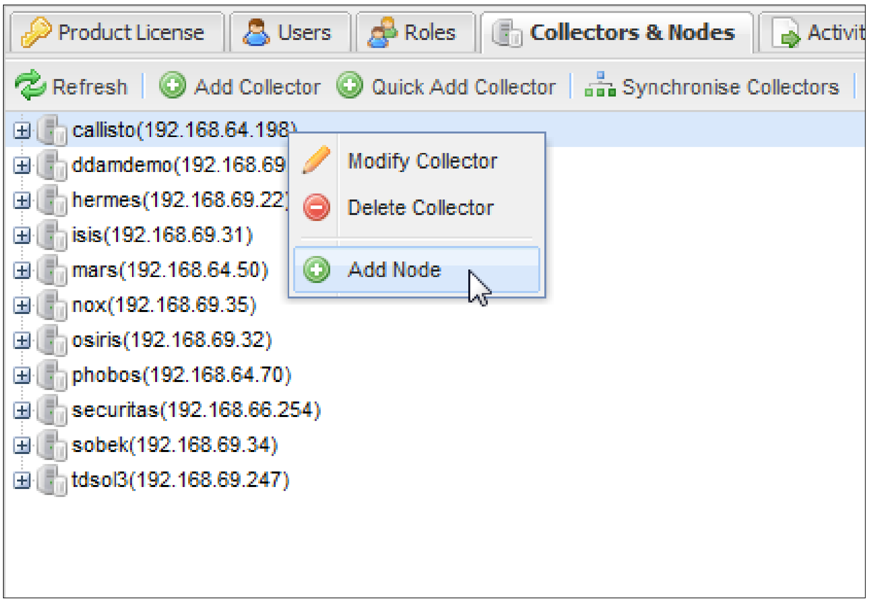
Name: callisto

IP Address: 192.168.64.198

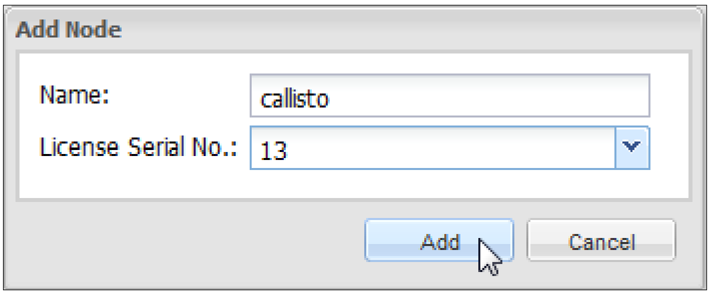
Buffer Activity Logs: ☐

Field	Description
Name	Name to assign to the collector (NOTE: This does not need to match the DNS name, it is merely a "friendly" name).
IP Address	IP Address of the host on which the collector agent has been installed. This needs to be reachable from the DDAM Master Server.
Buffer Activity Logs	Checking this box instructs the collector to buffer activity log writes to disk. This increases the performance of the collector process on high throughput collectors. However, checking this box means activity will not be displayed in real-time under the Activity pages for nodes associated with this collector.

Once the collector has been defined, it will appear within the "Collectors & Nodes" display. Using the right click menu, the collector can be selected and a node can be added by selecting "Add Node":



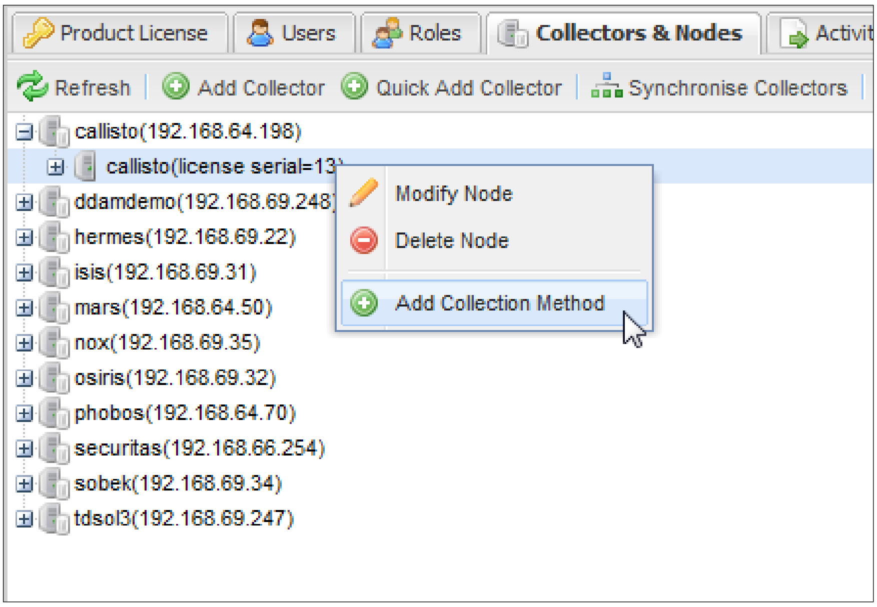
The "Add Node" dialogue box requires the name of the node to be entered a license serial number to be selected from the drop down list. If the node is going to be used for DNS/DHCP raw packet capture, then it is suggested that the node name be set the same as the collector name. If the node is going to be used for syslog traffic capture, then it is suggested that the node name be set to the name of the device that is generating the syslog traffic. This will make it easier to identify within the product.


Add Node

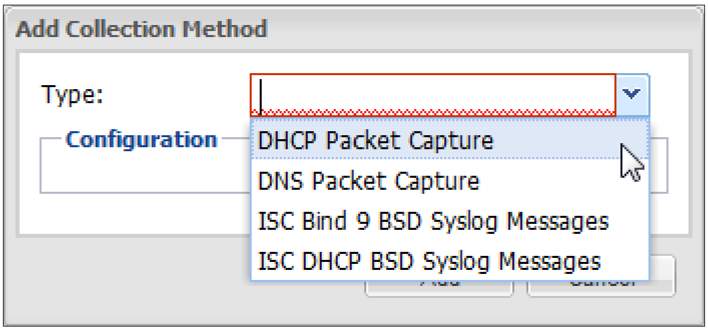
Name: callisto

License Serial No.: 13

Once the node has been defined, it will appear under the collector that it is attached to. Using the right click menu, the node can be selected and a collection method added by selecting "Add Collection Method":

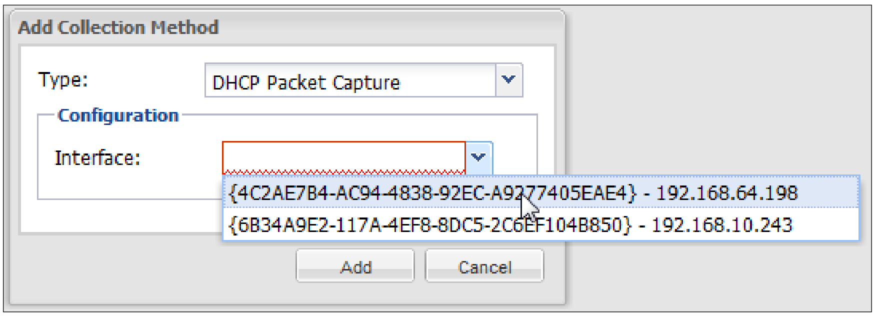


The "Add Collection Method" dialogue box enables the type of collection method to be specified. There are currently four collection methods available which will be listed when the "Type" drop down box is selected:



The Configuration area will vary dependent upon the collection method type and will prompt for additional information as required. The configuration fields for each type of collection method are explained below.

4.4.2.1 DHCP Packet Capture


Add Collection Method
Configuration
Interface:
{4C2AE7B4-AC94-4838-92EC-A9277405EAE4} - 192.168.64.198
{6B34A9E2-117A-4EF8-8DC5-2C6EF104B850} - 192.168.10.243
Add
Cancel

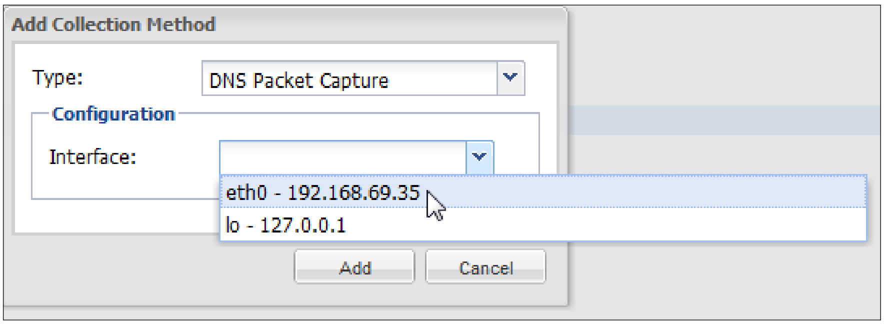
Type: DHCP Packet Capture

Configuration Field	Description
Interface	The network interface that packet capture should be performed on.

When selecting the interface drop down, the system will automatically detect the available network interfaces on the node and allow the user to select one. Depending on the operating system, the interface may be represented by different nomenclature. On Windows systems, the interface may be identified by a long hexadecimal unique identifier – however DDAM will append the interface IP address in order to make interface identification easier. On Unix/Linux systems, the interfaces will have names such as lo, eth0, eth1 etc. – DDAM again appends the IP address though.

If a node has multiple interfaces that all need to have packet capture enabled, additional collection methods can be added for each additional interface.

4.4.2.2 DNS Packet Capture



Type: DNS Packet Capture

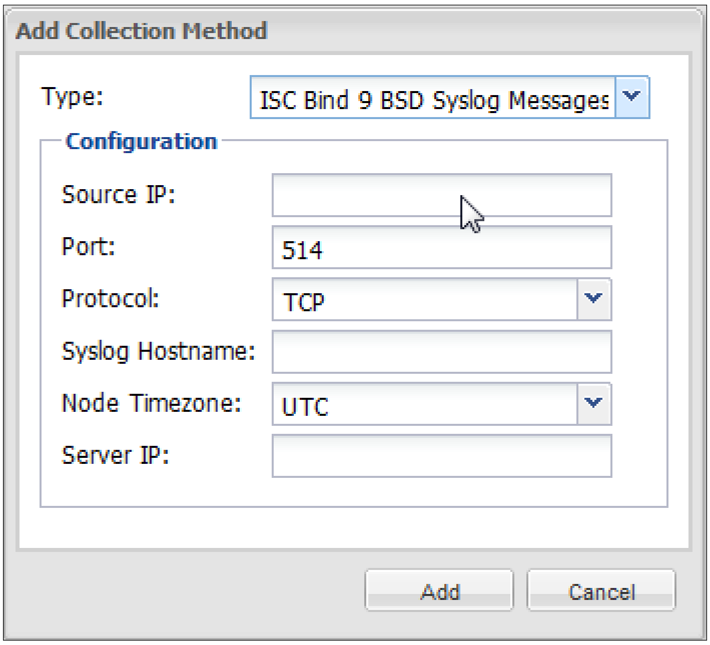
Interface:
- eth0 - 192.168.69.35
- lo - 127.0.0.1

Configuration Field	Description
Interface	The network interface that packet capture should be performed on.

When selecting the interface drop down, the system will automatically detect the available network interfaces on the node and allow the user to select one. Depending on the operating system, the interface may be represented by different nomenclature. On Windows systems, the interface may be identified by a long hexadecimal unique identifier – however DDAM will append the interface IP address in order to make interface identification easier. On Unix/Linux systems, the interfaces will have names such as lo, eth0, eth1 etc. – DDAM again appends the IP address though.

If a node has multiple interfaces that all need to have packet capture enabled, additional collection methods can be added for each additional interface.

4.4.2.3 ISC Bind 9 BSD Syslog Messages



Type: ISC Bind 9 BSD Syslog Messages

Source IP:

Port: 514

Protocol: TCP

Syslog Hostname:

Node Timezone: UTC

Server IP:

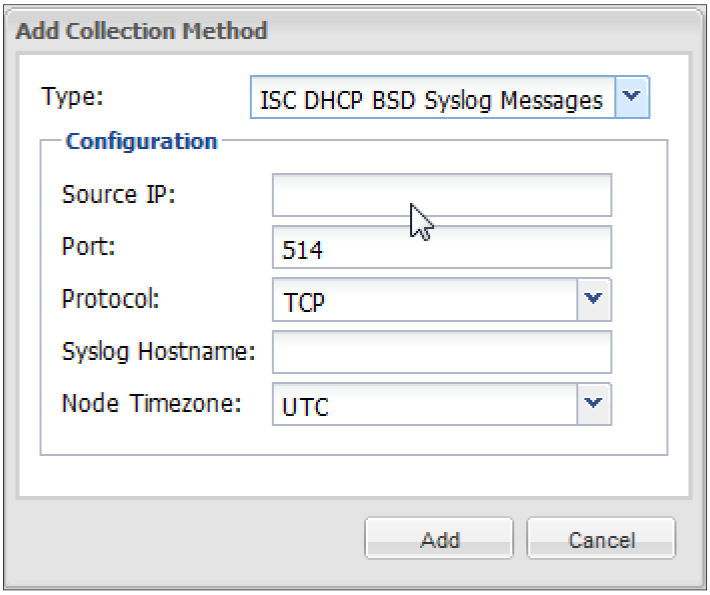
Configuration Field	Description
Source IP	The IP address of the system sending the syslog messages. Note, this may not be the actual DNS server being monitored, but could be a syslog server or concentrator that is used to collect syslog messages from many devices and forward the traffic on. This IP address is used to create an access control list to restrict syslog traffic only to this source IP address.
Port	The port number upon which to listen for syslog messages. The default value for syslog is 514 but it can be changed if required
Protocol	The network protocol that is being used by syslog, either UDP or TCP. TCP is the default and is more efficient than UDP, but not all devices support syslog over TCP. If using UDP, there is a danger that packets could be

	dropped on busy systems as UDP does not guarantee delivery of packets.
Syslog Hostname	This should match the host name that the DNS server writes into each syslog message. This is so that the correct syslog messages are processed when multiple servers are writing to the same syslog server or concentrator. If the syslog host name does not match the name being written by the server, no data will be collected. **NOTE:** Infoblox appliances typically use their IP address instead of the host name.
Node Time zone	The local time zone that the DNS server resides within. This is required because syslog produces time stamps based on the local time zone but does not indicate what the time zone is. When the syslog traffic is processed by the DDAM collector agent, it uses the "Node Time zone" setting to convert timestamps to UTC so that DNS servers in different time zones do not report timestamps that are in the future or the past.
Server IP	It is not be possible to determine the IP address of the DNS server from the syslog traffic. Enter the DNS server's IP address in this field. This is used to populate the "Server IP" field in the DNS Query Requests tab under the "Activity" icon.

In normal operation, syslog collection methods might typically be set up to use port 514 by default. The collector will then process all syslog traffic arriving at port 514 in a sequential manner. As the collector is also responsible for generating alerts, it is possible that in a busy environment it could take some time for the alert to be triggered due to the sequential nature of the processing.

In order to improve throughput, it is possible to configure syslog collection methods on different nodes to use different non-standard ports. The DNS servers that generate the syslog traffic will also need to be configured to send the syslog traffic to the non-standard port, but with traffic arriving on different ports the collector process is now able to process the traffic in parallel, thus improving throughput.

4.4.2.4 ISC DHCP BSD Syslog Messages


Add Collection Method

Type: ISC DHCP BSD Syslog Messages

Configuration

Source IP:

Port: 514

Protocol: TCP

Syslog Hostname:

Node Timezone: UTC

Configuration Field	Description
Source IP	The IP address of the system sending the syslog messages. Note, this may not be the actual DHCP server being monitored, but could be a syslog server or concentrator that is used to collect syslog messages from many devices and forward the traffic on. This IP address is used to create an access control list to restrict syslog traffic only to this source IP address.
Port	The port number upon which to listen for syslog messages. The default value for syslog is 514 but it can be changed if required.

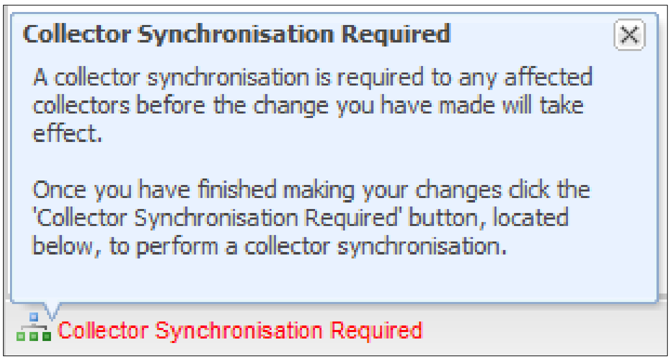
Protocol	The network protocol that is being used by syslog, either UDP or TCP. TCP is the default and is more efficient than UDP, but not all devices support syslog over TCP. If using UDP, there is a danger that packets could be dropped on busy systems as UDP does not guarantee delivery of packets.
Syslog Hostname	This should match the host name that the DHCP server writes into each syslog message. This is so that the correct syslog messages are processed when multiple servers are writing to the same syslog server or concentrator. If the syslog host name does not match the name being written by the server, no data will be collected. **NOTE:** Infoblox appliances typically use their IP address instead of the host name.
Node Time zone	The local time zone that the DNS server resides within. This is required because syslog produces time stamps based on the local time zone but does not indicate what the time zone is. When the syslog traffic is processed by the DDAM collector agent, it uses the "Node Time zone" setting to convert timestamps to UTC so that DNS servers in different time zones do not report timestamps that are in the future or the past.

4.4.3 Collector Synchronization

A collector synchronization is required whenever any changes are made under the "Collectors & Nodes" tab (they are also required when the product license, external systems or alerts are configured).

A collector synchronization distributes the changes necessary to the relevant collectors and automatically determines which collectors require synchronization and also whether the collector process needs to be restarted.

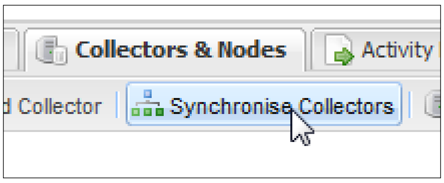
A collector synchronization can either be initiated by the "Collector Synchronization Required" button when it has turned red in color, or via the "Synchronize Collectors" button on the toolbar under the "Collectors & Nodes" tab:



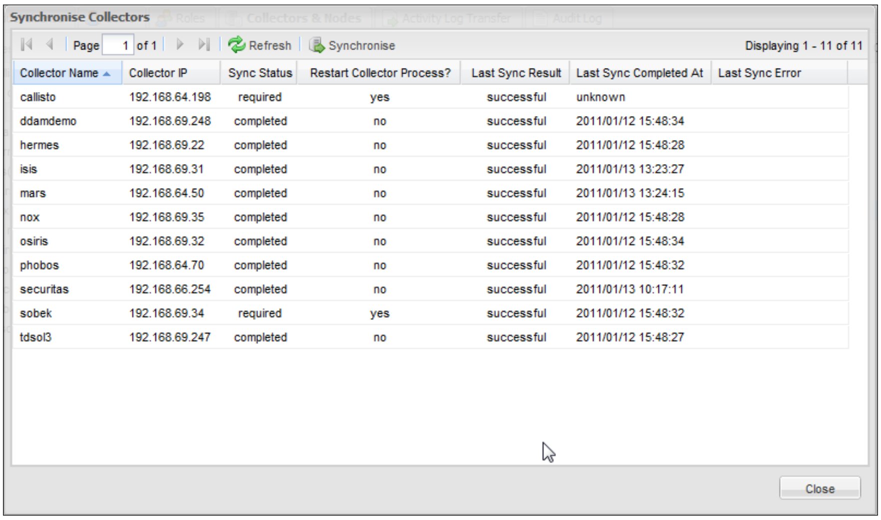
Collector Synchronisation Required

A collector synchronisation is required to any affected collectors before the change you have made will take effect.

Once you have finished making your changes click the 'Collector Synchronisation Required' button, located below, to perform a collector synchronisation.

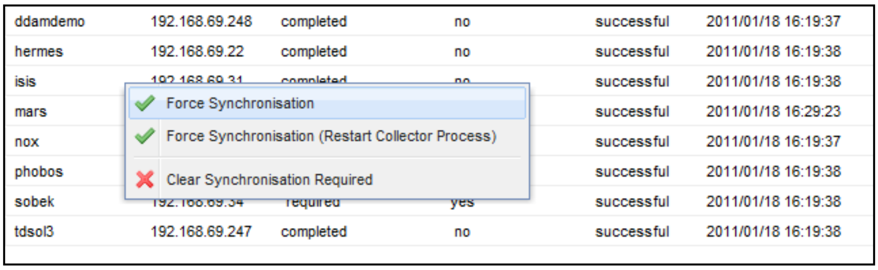


After selecting either the "Collector Synchronization Required" button or the "Synchronize Collectors" button, the synchronize collectors screen is displayed:



Collector Name	Collector IP	Sync Status	Restart Collector Process?	Last Sync Result	Last Sync Completed At	Last Sync Error
callisto	192.168.64.198	required	yes	successful	unknown	
ddamdemo	192.168.69.248	completed	no	successful	2011/01/12 15:48:34	
hermes	192.168.69.22	completed	no	successful	2011/01/12 15:48:28	
isis	192.168.69.31	completed	no	successful	2011/01/13 13:23:27	
mars	192.168.64.50	completed	no	successful	2011/01/13 13:24:15	
nox	192.168.69.35	completed	no	successful	2011/01/12 15:48:28	
osiris	192.168.69.32	completed	no	successful	2011/01/12 15:48:34	
phobos	192.168.64.70	completed	no	successful	2011/01/12 15:48:32	
securitas	192.168.66.254	completed	no	successful	2011/01/13 10:17:11	
sobek	192.168.69.34	required	yes	successful	2011/01/12 15:48:32	
tdsol3	192.168.69.247	completed	no	successful	2011/01/12 15:48:27	

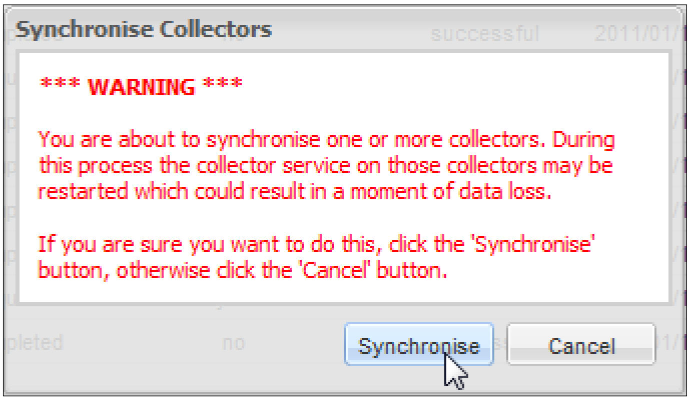
This screen details when the last successful synchronization occurred and if there was an error what the error message was. In certain cases it may be necessary to force a synchronization and/or collector process restart, for instance if recovering a collector from backup. This can be achieved by selecting the relevant collector and then using the right click menu to specify whether a synchronization and/or collector process restart is required:



ddamdemo	192.168.69.248	completed	no	successful	2011/01/18 16:19:37
hermes	192.168.69.22	completed	no	successful	2011/01/18 16:19:38
isis	192.168.69.31	completed	no	successful	2011/01/18 16:19:38
mars				successful	2011/01/18 16:29:23
nox				successful	2011/01/18 16:19:37
phobos				successful	2011/01/18 16:19:38
sobek	192.168.69.34	required	yes	successful	2011/01/18 16:19:38
tdsol3	192.168.69.247	completed	no	successful	2011/01/18 16:19:38

Force Synchronisation
Force Synchronisation (Restart Collector Process)
Clear Synchronisation Required

Clicking the "Synchronize" button displays a warning stating that any collectors that require a restart may experience a small amount of data loss while the collector process is restarted.

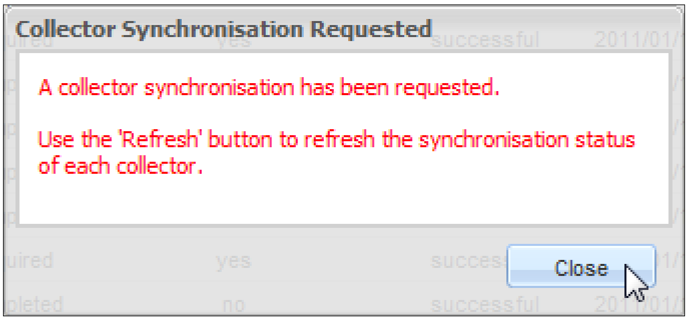


*** WARNING ***

You are about to synchronise one or more collectors. During this process the collector service on those collectors may be restarted which could result in a moment of data loss.

If you are sure you want to do this, click the 'Synchronise' button, otherwise click the 'Cancel' button.

After pressing "Synchronize" another dialogue box confirms that a collector synchronization has been requested:



Collector Synchronisation Requested

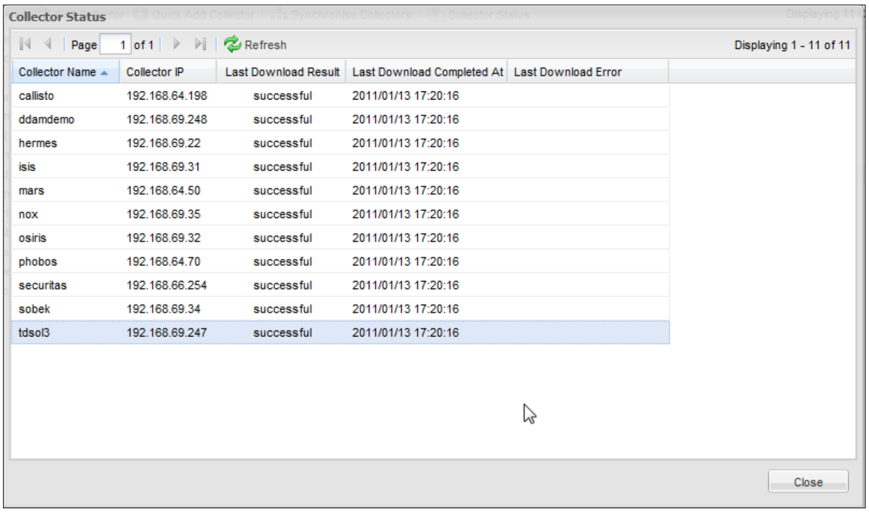
A collector synchronisation has been requested.

Use the 'Refresh' button to refresh the synchronisation status of each collector.

Collector synchronization occurs in the background, and the synchronize collectors display will list the state of each collector that requires synchronization. Clicking "Refresh" will update the display.

4.4.4 Collector Status

The DDAM master server communicates with each collector in sequence and periodically downloads alert and report data. The status of these downloads can be viewed by using the "Collector Status" display:



Collector Status

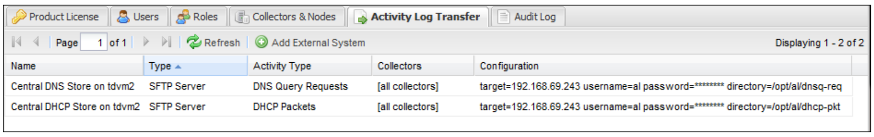
Collector Name	Collector IP	Last Download Result	Last Download Completed At	Last Download Error
callisto	192.168.64.198	successful	2011/01/13 17:20:16	
ddamdemo	192.168.69.248	successful	2011/01/13 17:20:16	
hermes	192.168.69.22	successful	2011/01/13 17:20:16	
isis	192.168.69.31	successful	2011/01/13 17:20:16	
mars	192.168.64.50	successful	2011/01/13 17:20:16	
nox	192.168.69.35	successful	2011/01/13 17:20:16	
osiris	192.168.69.32	successful	2011/01/13 17:20:16	
phobos	192.168.64.70	successful	2011/01/13 17:20:16	
securitas	192.168.66.254	successful	2011/01/13 17:20:16	
sobek	192.168.69.34	successful	2011/01/13 17:20:16	
tdsol3	192.168.69.247	successful	2011/01/13 17:20:16	

The "Last Download Result" should indicate if there are any problems, and the "Last Download Completed At" column will display when the last download occurred. Any collectors that do not have a recent date/time in this column are likely experiencing an issue and require investigation.

4.5 Activity Log Transfer

DDAM can transfer DNS and DHCP activity logs to external systems for security, archiving or custom reporting purposes. Archiving the activity log data means it can still be searched even if the data is no longer present within DDAM.

Activity log transfers can be configured under the Configure->Activity Log Transfer page.



Name	Type	Activity Type	Collectors	Configuration
Central DNS Store on tdvm2	SFTP Server	DNS Query Requests	[all collectors]	target=192.168.69.243 username=al password=******** directory=/opt/al/dnsq-req
Central DHCP Store on tdvm2	SFTP Server	DHCP Packets	[all collectors]	target=192.168.69.243 username=al password=******** directory=/opt/al/dhcp-pkt

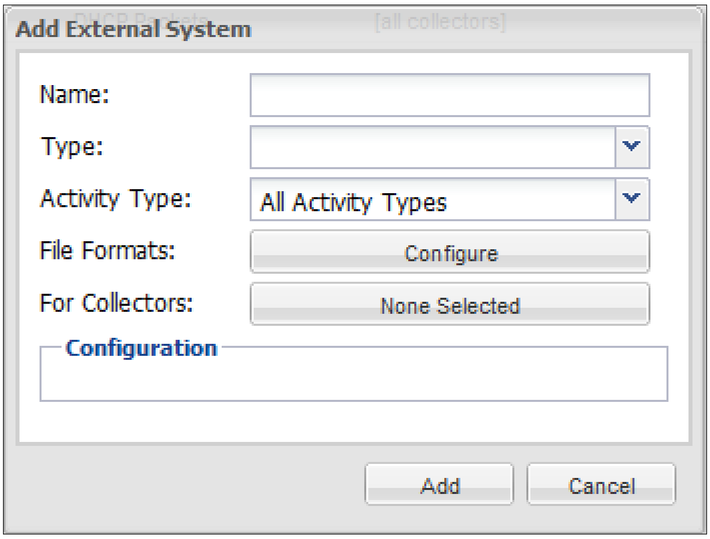
Under this page, external systems can be configured on a per Collector basis using different file transfer protocols. By default, activity logs are "rolled" every 10 minutes to keep them at a manageable size and the transfer process checks every 60 seconds for newly rolled logs. Therefore the activity log transfer will typically occur every 10 minutes.

Each external system defined is displayed with the following columns:

Column	Description
Name	Name of the external system.
Type	Type of external system.
Activity Type	What type of activity will be transferred to the external system.
Collectors	A list of Collectors the external system is configured for.
Configuration	A list of key/value pairs detailing the configuration of the external system. The contents of this field will be different for each type of external system.

External systems can be added by clicking the "Add External System" button. Existing external system configurations can be modified or deleted using the right click menu.

After pressing the "Add External System" button, a dialogue box is displayed where the external system can be configured:



Name:

Type:

Activity Type: All Activity Types

File Formats:

For Collectors: None Selected

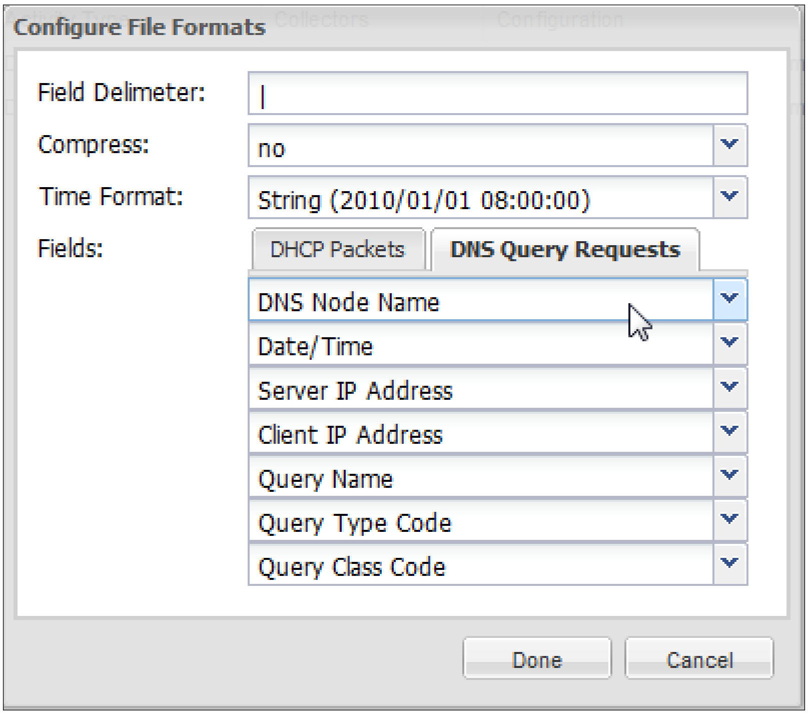
The following fields can be configured when adding and modifying an external system:

Field	Description
Name	Name of the external system.
Type	Type of external system to add. Currently the system supports "FTP" and "SFTP" file transfer mechanisms, or can write to a local directory on each collector.
Activity Type	The type of activity logs should that be transferred to the external system (DNS, DHCP or All).
File Formats	Specifies how activity logs should be formatted before they are transferred to external systems. Refer to the Transfer File Format section for

	more information on configuring the file formats.
For Collectors	Specifies which Collectors this external system should be configured for.
Configuration	This field set will contain a number of configurable options relevant to the type of external system that was added in the Type field.

4.5.1 Transfer File Format

When configuring external systems, the format of the data can be specified before it is transferred. Items that can be configured include the delimiter that is used to separate fields, the format of the time stamp field and which fields are exported and what order they are exported in. The transfer file format is configured using the File Formats button when adding or modifying an external system.



Configure File Formats

Field Delimeter: |

Compress: no

Time Format: String (2010/01/01 08:00:00)

Fields:

DNS Node Name

Date/Time

Server IP Address

Client IP Address

Query Name

Query Type Code

Query Class Code

The following options can be configured for the transfer file format:

Options	Description
Field Delimiter	How fields in activity logs should be delimited. Something that is not commonly used within DNS queries should be used as a delimiter, i.e. the pipe symbol "|", or hat symbol "^". Commas "," should not generally be used as a delimiter as they are sometimes seen in DNS queries.
Compress	Whether to compress activity logs using GZIP. Compressing the logs will make them harder to search as they will need to be uncompressed first but will save disk space.
Time Format	Specifies how time the date/time field in activity logs should be formatted. "ctime" is the number of elapsed seconds since midnight January 1, 1970 UTC and is useful if the logs are being processed by scripts. "String" is the date/time in human readable format "YYYY/MM/DD HH:MM:SS" in the local time of the collector.
Fields	One or more tabs will be displayed allowing the fields to be included/excluded or re-ordered. Select "-" to exclude a field.

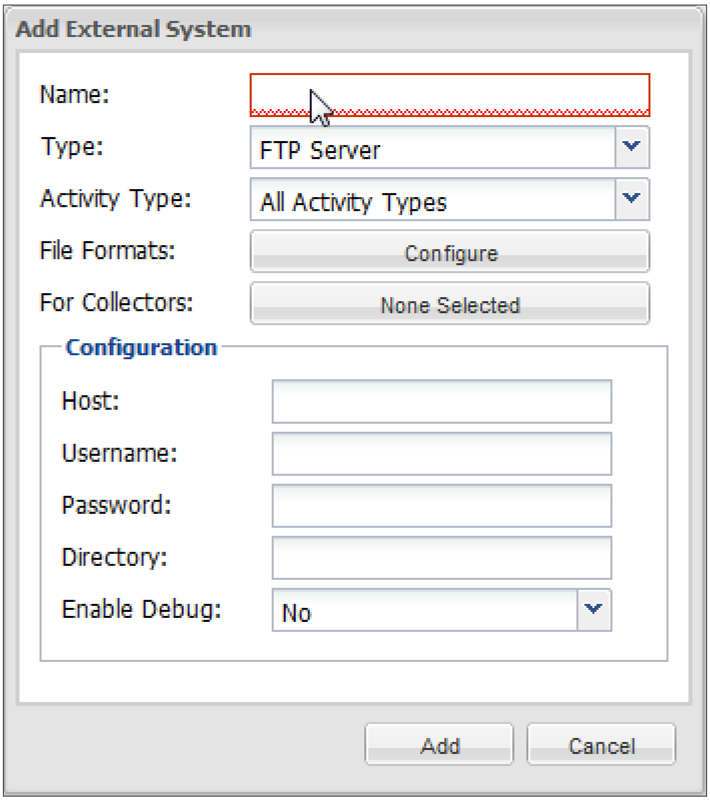
4.5.2 Available External Systems

The following external system types can be configured:

4.5.2.1 FTP Server

Activity logs will be transferred to external systems using the File Transfer Protocol (FTP) into a configured directory.

FTP uses plain text passwords to connect to the destination server and no encryption is performed on the data. If encrypted passwords and/or encryption of the data transfer is required, use the "SFTP Server" option.



Add External System

Name:

Type: FTP Server

Activity Type: All Activity Types

File Formats: Configure

For Collectors: None Selected

Configuration

Host:

Username:

Password:

Directory:

Enable Debug: No

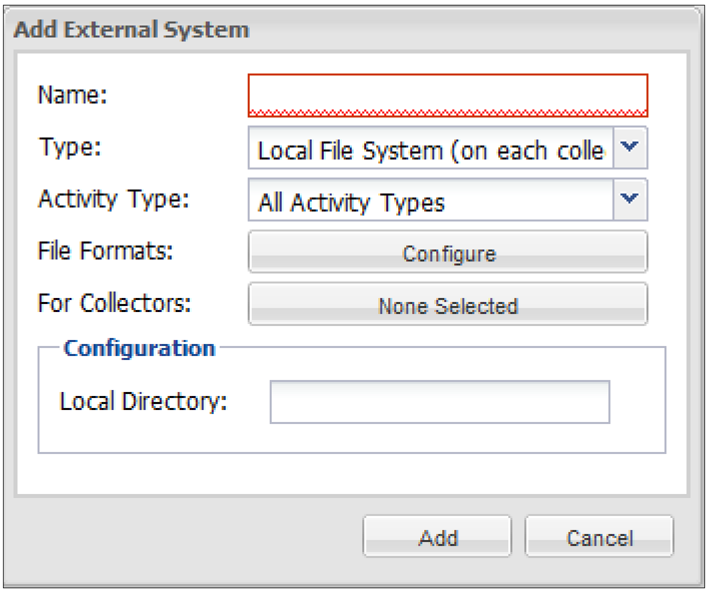
The following configurable options are available for this external system:

Option	**Description**
Host	IP address or hostname of the target FTP server.
Username	Username which will be used to login to the FTP server.
Password	Password for the configured FTP user.
Directory	Directory into which activity logs should be placed (this must already exist).
Enable Debug	This is used by support for troubleshooting

	purposes.

4.5.2.2 Local File System

Activity logs will be placed into a local directory on each Collector (the directory must already exist).



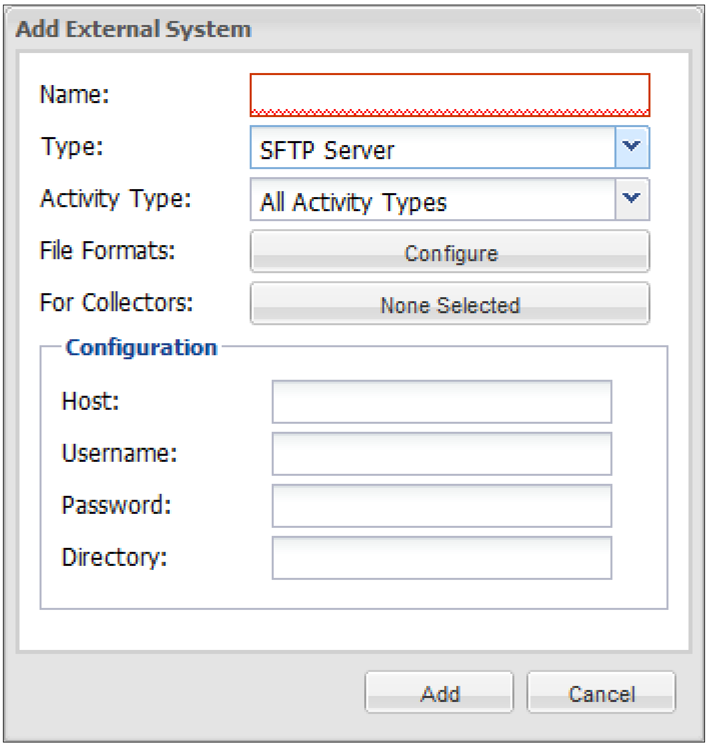
The following configurable options are available for this alerting method:

Option	Description
Local Directory	The full path to the directory into which activity logs should be placed. **NOTE:** This could reside on a NFS mounted file system or Windows mapped drive letter.

4.5.2.3 SFTP Server

Activity logs will be transferred to external systems using the Secure File Transfer Protocol (SFTP) into a configured directory.

The advantage of using SFTP is that all passwords and data are encrypted using SSH (Secure Shell), however the server must support SFTP in order to use it.

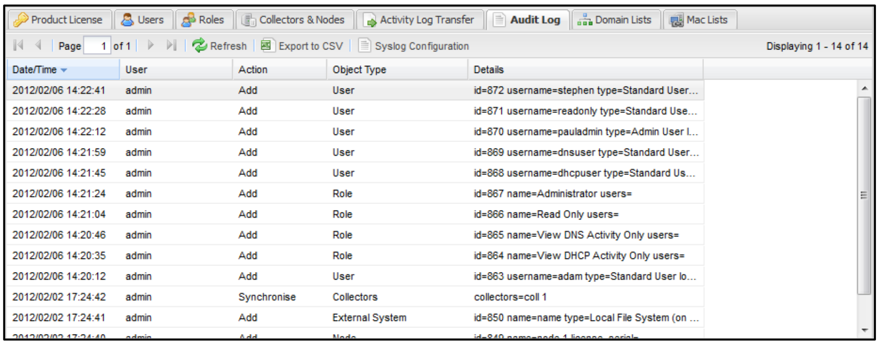


The following configurable options are available for this external system:

Option	Description
Host	IP address or hostname of the target SFTP server.
Username	Username which will be used to login to the SFTP server.
Password	Password for the configured SFTP user.
Directory	Directory into which activity logs should be placed (this must already exist).

4.6 Audit Log

Any changes made within DDAM are logged in the systems audit log. Audit events can be viewed under the Configure->Audit Log page.



Date/Time	User	Action	Object Type	Details
2012/02/06 14:22:41	admin	Add	User	id=872 username=stephen type=Standard User...
2012/02/06 14:22:28	admin	Add	User	id=871 username=readonly type=Standard Use...
2012/02/06 14:22:12	admin	Add	User	id=870 username=pauladmin type=Admin User l...
2012/02/06 14:21:59	admin	Add	User	id=869 username=dnsuser type=Standard User...
2012/02/06 14:21:45	admin	Add	User	id=868 username=dhcpuser type=Standard Us...
2012/02/06 14:21:24	admin	Add	Role	id=867 name=Administrator users=
2012/02/06 14:21:04	admin	Add	Role	id=866 name=Read Only users=
2012/02/06 14:20:46	admin	Add	Role	id=865 name=View DNS Activity Only users=
2012/02/06 14:20:35	admin	Add	Role	id=864 name=View DHCP Activity Only users=
2012/02/06 14:20:12	admin	Add	User	id=863 username=adam type=Standard User lo...
2012/02/02 17:24:42	admin	Synchronise	Collectors	collectors=coll 1
2012/02/02 17:24:41	admin	Add	External System	id=850 name=name type=Local File System (on ...

On this page, events can be searched (using filters) and exported. The following columns are displayed under this page:

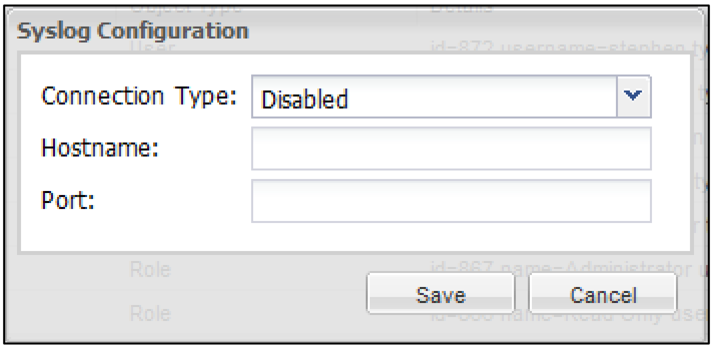
Column	Filter Type	Description
Date/Time	Date/Time	Date and time the event was logged.
User	String	User which triggered the event.
Action	String	What action the user performed.
Object Type	String	What type of object the user invoked an action on.
Details	String	A list of key/value pairs giving details about the parameters for the event.

4.6.1 Syslog

Optionally audit events may be logged to either a local or a remote syslog server. If DDAM is installed on a Microsoft Windows platform, the local Microsoft Windows Event Log will be used instead.

Instead of a local syslog server, audit events can be forwarded to a remote syslog server using either UDP or TCP.

Syslog configuration can be managed from the “Audit Log” tab by clicking the “Syslog Configuration” button:



Syslog Configuration

Connection Type: Disabled

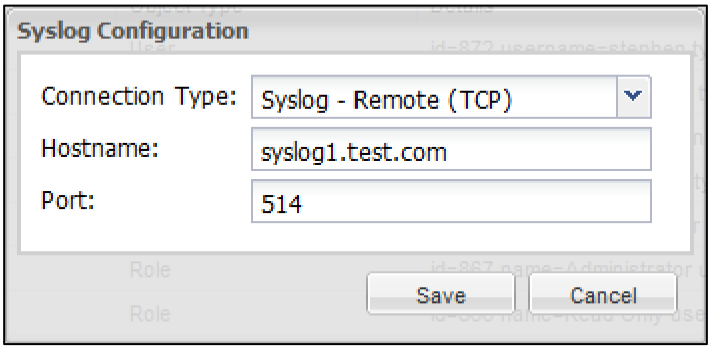
Hostname:

Port:

The following are supported connection types:

Connection Type	Description
Disabled	Audit events are not forwarded.
Syslog - Remote (TCP)	Audit events are forwarded to a remote syslog server via TCP.
Syslog - Remote (UDP)	Audit events are forwarded to a remote syslog server via UDP.
MS Windows Eventlog - Local	Audit events are written to the Windows Application Event Log on the Master.
Syslog - Local	Audit events are written to syslog daemon on the Master.

When a remote connection type is selected the hostname and port options can be configured:



Connection Type: Syslog - Remote (TCP)
Hostname: syslog1.test.com
Port: 514

4.7 Domain Lists

Domain Lists provide a way to group a list of related domains so that they may be specified elsewhere in DDAM as a single entity, e.g. a list of known bad domains (or blacklisted domains) or a list of internal domains. Domain Lists can be created from scratch by the end-user, or they can be generated by other systems, such as SIEM, IDS/IPS or firewall systems.

Domain Lists are useful for monitoring malware, botnets and queries for malicious domains. Various organizations publish malware domain lists that can be downloaded from the Internet and uploaded into DDAM. Examples of publicly available malware domain lists are:

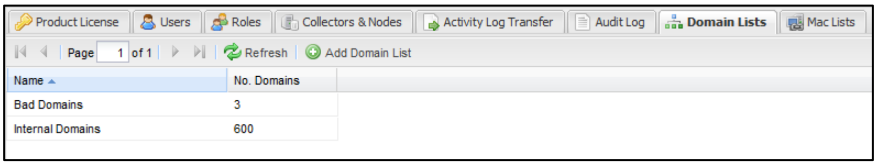
http://www.malwaredomainlist.com/hostslist/hosts.txt

https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist

http://winhelp2002.mvps.org/hosts.txt

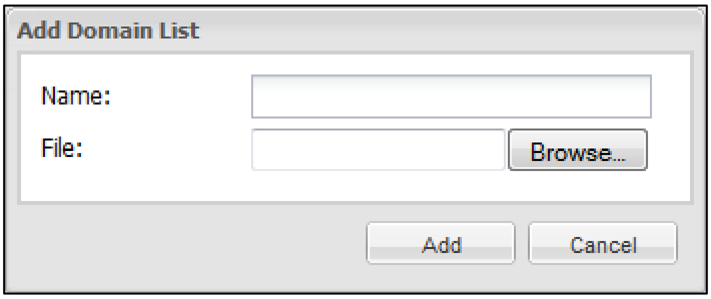
NOTE: Domain Lists are currently supported by the alerting feature in DDAM. Support for other features, such as reporting, are planned.

Domain Lists are configured under the “Domain Lists” tab:



Name	No. Domains
Bad Domains	3
Internal Domains	600

Domain Lists can be added by clicking the “Add Domain List” button:



After entering a descriptive name for the Domain List (e.g. "Malicious domains", "Internal domains" etc.), specify the file name of the text file containing the domain list by clicking the "Browse" button and click the “Add” button to finish defining the domain list.

Domain List files are simply text files containing lines similar to the following:

```
##
## these are comments
##

*.one.com
www.*
127.0.0.1 TWO.COM
three.com 127.0.0.1
four.com 127.0.0.1 # this is a comment
five.com  # this is another comment
six.com
```

The following rules summarize the format:

- On each line, any text following, and including, the “#” character is treated as a comment and ignored
- White space is ignored (i.e. tabs and spaces are treated the same, empty lines are also ignored)
- Lines can contain a domain name with an optional IP address separated by white space (IP addresses are ignored but can appear in the file for administrational purposes)
- IP addresses can appear before domain names (i.e. “192.168.2.100 domain.com” instead of “domain.com 192.168.2.100”)
- Domain names are case-insensitive
- Domains can contain one wildcard using the “*” character either at the beginning or end (e.g. “*.domain.com” or “www.*”)

An implicit wildcard is added to any domain where a wildcard was not explicitly specified to match domain apex and sub-domain queries. For example, the domain “domain.com”, in a Domain List file, will expand to match “domain.com” and “*.domain.com” once loaded by the alerting engine.

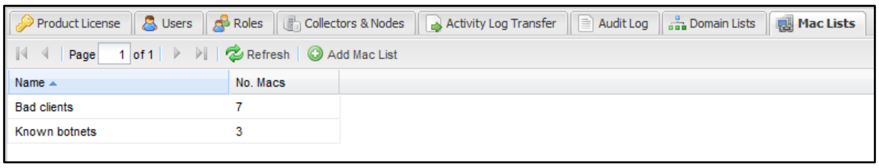
Once a Domain List file has been uploaded it cannot be edited. To edit or replace the contents of a Domain List file you must download (by right clicking the Domain List and selecting “Download Domain List”), edit, and then upload (by right clicking the Domain List and selecting “Modify Domain List”).

4.8 MAC Lists

Like Domain Lists, MAC Lists provide a way to group a list of related MAC addresses (or end devices) so that they may be specified elsewhere in DDAM as a single entity, e.g. a list of known bad clients.

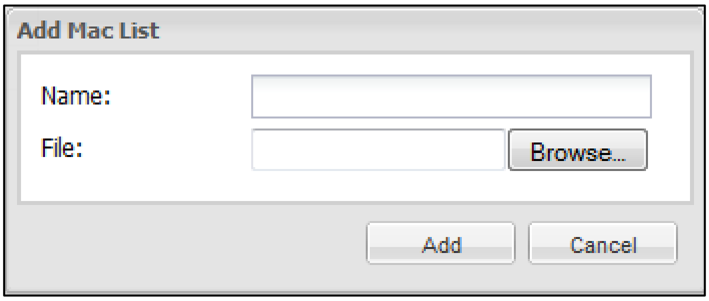
NOTE: MAC Lists are currently supported by the alerting feature in DDAM. Support for other features, such as reporting, are planned.

MAC Lists are configured under the “MAC Lists” tab:



Name	No. Macs
Bad clients	7
Known botnets	3

MAC Lists can be added by clicking the “Add MAC List” button:



After entering a descriptive name for the MAC List, specify the file name of the text file containing the MAC list by clicking the "Browse" button and click the “Add” button to finish defining the MAC list.

MAC List files are simply text files containing lines similar to the following:

```
##
## these are comments
##

*111111
222222*
333333333333
*44:44:44
55:55:55:55:55:55 # this is a comment
6666.6666.6666
77-77-77-77-77-77
```

The following rules summarize the format:

- On each line, any text following, and including, the “#” character is treated as a comment and ignored
- White space is ignored (i.e. tabs and spaces are treated the same, empty lines are also ignored)
- Lines can contain one MAC address expressed in hexadecimal notation in the form of “xxxxxxxxxxxx”, “xx:xx:xx:xx:xx:xx”, “xx-xx-xx-xx-xx-xx” or “xxxx.xxxx.xxxx”
- Hexadecimal characters in MAC addresses are case-insensitive
- MAC addresses can contain one wildcard using the “*” character either at the beginning or end (e.g. “00295c*” or “*f4”)

Once a MAC List file has been uploaded it cannot be edited. To edit or replace the contents of a MAC List file you must download (by right clicking the MAC List and selecting “Download MAC List”), edit, and then upload (by right clicking the MAC List and selecting “Modify MAC List”).

Chapter

5

5 Activity View

The activity view is accessed by clicking the Activity icon.

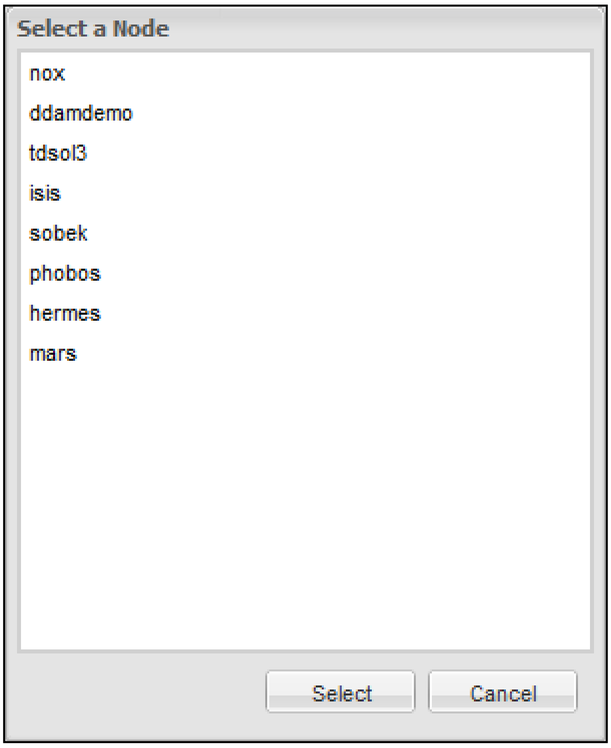
Activity

NOTE: If the appropriate permissions have not been given this icon will not be displayed.

The activity view provides users with access to real-time DNS and DHCP activity. This can be used for troubleshooting and support.

An approximate 1 hour sliding window of activity is kept. To keep more data, the Activity Log Transfer feature should be used to archive activity to an external system. More information regarding Activity Log Transfers can be found in section 4.5.

Activity is viewed on a per-node basis. On first navigation to the activity view, the user will be prompted to select a node. Simply select the node and click the "Select" button.



Note, when first logging into the system, the "DHCP Packets" tab is selected by default. If the user wishes to view DNS activity rather than DHCP activity, simply selecting "Cancel" will enable the "DNS Query Requests" tab to be selected and a DNS node specified.

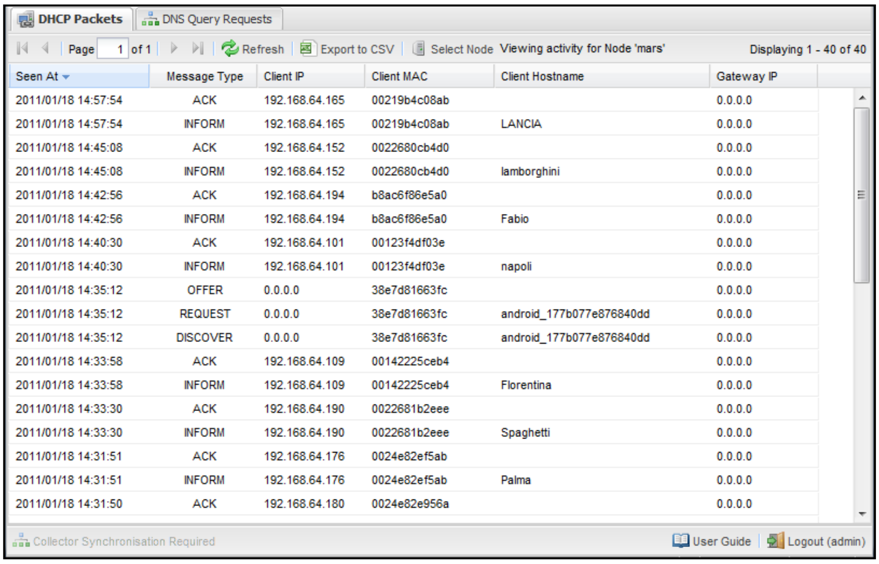
At any point a different node can be selected by clicking the "Select Node" button in the toolbar.

5.1 DHCP Packet Activity

DHCP packet activity can be viewed by clicking the "DHCP Packets" tab. After selecting a node, the following columns are displayed:

Column	Filter Type	Description
Seen At	Date/Time	At what time the activity was seen.

Message Type	Enum	ASCII representation of the DHCP message type code found in option 53 of the DHCP packet (e.g. DISCOVER, OFFER, REQUEST, ACK etc.). If option 53 was not present in the DHCP packet this field will be displayed as "0". If the type code in option 53 is not understood by DDAM this field will display the code. Available message types can be found in appendix A.
Client IP	IP Address	The value of the ciaddr (Client IP Address) field.
Client MAC	String	The value of the chaddr (Client Hardware Address) field.
Client Hostname	String	The value of the option 12 (hostname), if found.
Gateway IP	IP Address	The value of the giaddr (Gateway IP Address) field.



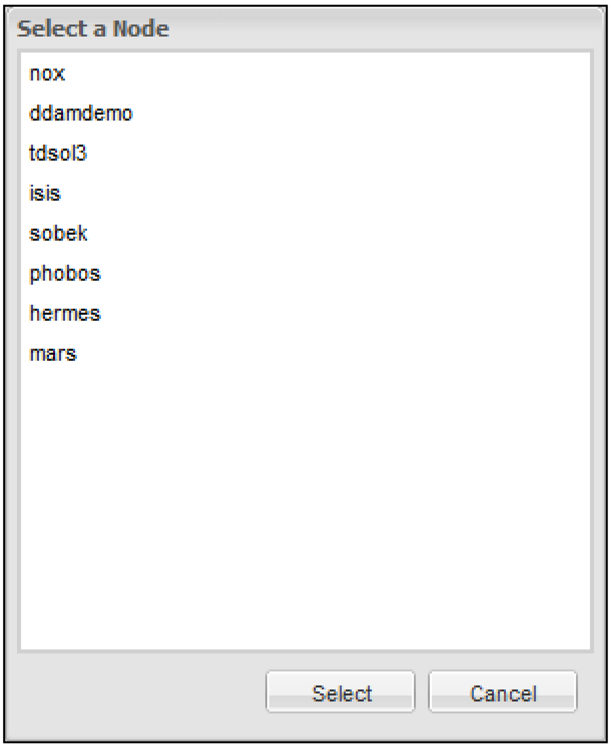
Viewing activity for Node 'mars'

Displaying 1 - 40 of 40

Seen At	Message Type	Client IP	Client MAC	Client Hostname	Gateway IP
2011/01/18 14:57:54	ACK	192.168.64.165	00219b4c08ab		0.0.0.0
2011/01/18 14:57:54	INFORM	192.168.64.165	00219b4c08ab	LANCIA	0.0.0.0
2011/01/18 14:45:08	ACK	192.168.64.152	0022680cb4d0		0.0.0.0
2011/01/18 14:45:08	INFORM	192.168.64.152	0022680cb4d0	lamborghini	0.0.0.0
2011/01/18 14:42:56	ACK	192.168.64.194	b8ac6f86e5a0		0.0.0.0
2011/01/18 14:42:56	INFORM	192.168.64.194	b8ac6f86e5a0	Fabio	0.0.0.0
2011/01/18 14:40:30	ACK	192.168.64.101	00123f4df03e		0.0.0.0
2011/01/18 14:40:30	INFORM	192.168.64.101	00123f4df03e	napoli	0.0.0.0
2011/01/18 14:35:12	OFFER	0.0.0.0	38e7d81663fc		0.0.0.0
2011/01/18 14:35:12	REQUEST	0.0.0.0	38e7d81663fc	android_177b077e876840dd	0.0.0.0
2011/01/18 14:35:12	DISCOVER	0.0.0.0	38e7d81663fc	android_177b077e876840dd	0.0.0.0
2011/01/18 14:33:58	ACK	192.168.64.109	00142225ceb4		0.0.0.0
2011/01/18 14:33:58	INFORM	192.168.64.109	00142225ceb4	Florentina	0.0.0.0
2011/01/18 14:33:30	ACK	192.168.64.190	0022681b2eee		0.0.0.0
2011/01/18 14:33:30	INFORM	192.168.64.190	0022681b2eee	Spaghetti	0.0.0.0
2011/01/18 14:31:51	ACK	192.168.64.176	0024e82ef5ab		0.0.0.0
2011/01/18 14:31:51	INFORM	192.168.64.176	0024e82ef5ab	Palma	0.0.0.0
2011/01/18 14:31:50	ACK	192.168.64.180	0024e82e956a		0.0.0.0

The system remembers which node is currently selected for the DHCP Packets tab, so if other operations are performed, and the DHCP Packets tab re-selected at a later date, the system will still display activity from the currently selected node.

To view DHCP activity from another node, this can be achieved by pressing the "Select Node" button and selecting a new node from the list.

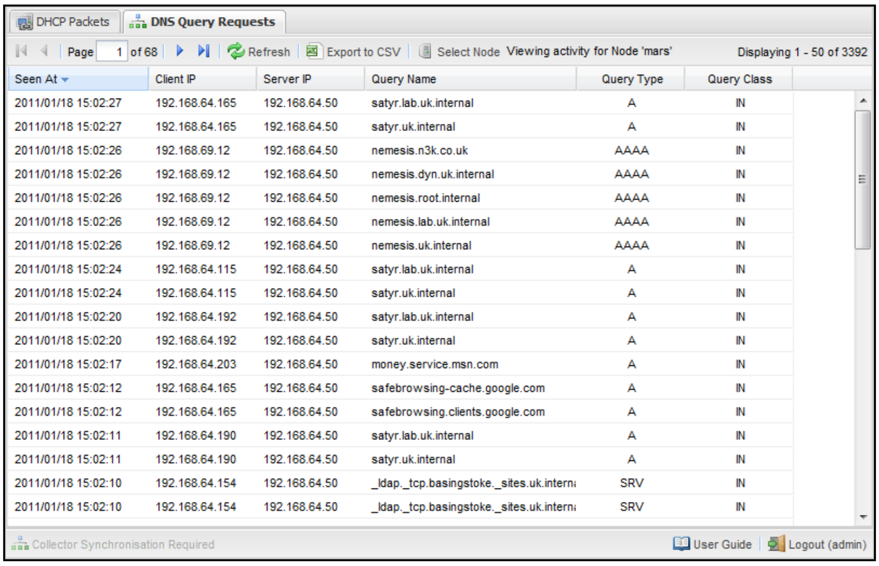


5.2 DNS Query Request Activity

DNS query request activity can be viewed by clicking the "DNS Query Requests" tab. After selecting a node, the following columns are displayed:

Column	Filter Type	Description
Seen At	Date/Time	At what time the activity was seen.

Server IP	IP Address	DNS server IP address.
Client IP	IP Address	DNS client IP address.
Query Name	String	Fully qualified domain name contained within the query.
Query Type	Enum	ASCII representation of the query type code (e.g. A, PTR, CNAME etc.). Available query types can be found in appendix B. If the type code is not understood by DDAM this field will display the code.
Query Class	Enum	ASCII representation of the query class code (e.g. IN, CS etc.). Available query classes can be found in appendix C. If the class code is not understood by DDAM this field will display the code.



Viewing activity for Node 'mars'

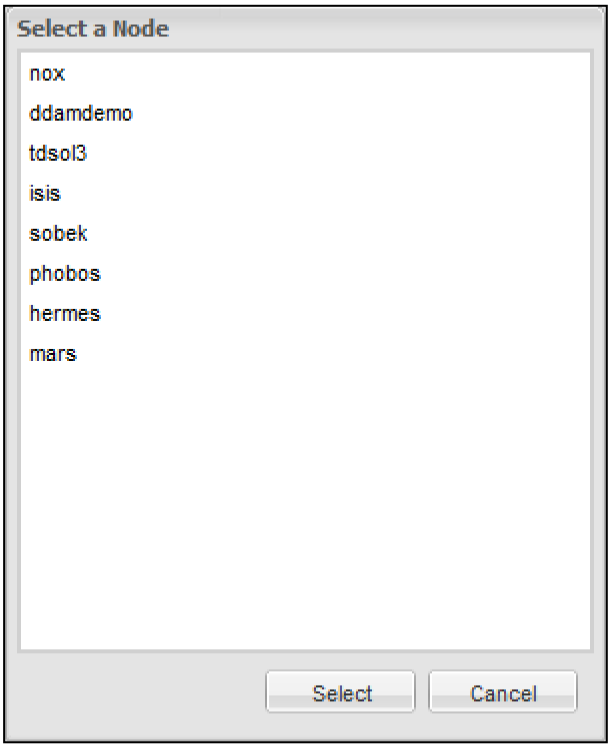
Displaying 1 - 50 of 3392

Seen At	Client IP	Server IP	Query Name	Query Type	Query Class
2011/01/18 15:02:27	192.168.64.165	192.168.64.50	satyr.lab.uk.internal	A	IN
2011/01/18 15:02:27	192.168.64.165	192.168.64.50	satyr.uk.internal	A	IN
2011/01/18 15:02:26	192.168.69.12	192.168.64.50	nemesis.n3k.co.uk	AAAA	IN
2011/01/18 15:02:26	192.168.69.12	192.168.64.50	nemesis.dyn.uk.internal	AAAA	IN
2011/01/18 15:02:26	192.168.69.12	192.168.64.50	nemesis.root.internal	AAAA	IN
2011/01/18 15:02:26	192.168.69.12	192.168.64.50	nemesis.lab.uk.internal	AAAA	IN
2011/01/18 15:02:26	192.168.69.12	192.168.64.50	nemesis.uk.internal	AAAA	IN
2011/01/18 15:02:24	192.168.64.115	192.168.64.50	satyr.lab.uk.internal	A	IN
2011/01/18 15:02:24	192.168.64.115	192.168.64.50	satyr.uk.internal	A	IN
2011/01/18 15:02:20	192.168.64.192	192.168.64.50	satyr.lab.uk.internal	A	IN
2011/01/18 15:02:20	192.168.64.192	192.168.64.50	satyr.uk.internal	A	IN
2011/01/18 15:02:17	192.168.64.203	192.168.64.50	money.service.msn.com	A	IN
2011/01/18 15:02:12	192.168.64.165	192.168.64.50	safebrowsing-cache.google.com	A	IN
2011/01/18 15:02:12	192.168.64.165	192.168.64.50	safebrowsing.clients.google.com	A	IN
2011/01/18 15:02:11	192.168.64.190	192.168.64.50	satyr.lab.uk.internal	A	IN
2011/01/18 15:02:11	192.168.64.190	192.168.64.50	satyr.uk.internal	A	IN
2011/01/18 15:02:10	192.168.64.154	192.168.64.50	_ldap._tcp.basingstoke._sites.uk.intern	SRV	IN
2011/01/18 15:02:10	192.168.64.154	192.168.64.50	_ldap._tcp.basingstoke._sites.uk.intern	SRV	IN

Collector Synchronisation Required

The system remembers which node is currently selected for the DNS Query Requests tab, so if other operations are performed, and the DNS Query Requests tab re-selected at a later date, the system will still display activity from the currently selected node.

To view DNS activity from another node, this can be achieved by pressing the "Select Node" button and selecting a new node from the list.

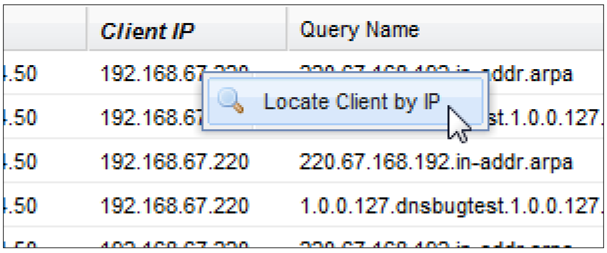


5.3 Client Location

DDAM supports a client location feature which allows an inventory system (e.g. porttracker or PortIQ) to be integrated with DDAM. This feature enables an administrator to physically locate a DNS or DHCP client on a switch port by IP address or MAC address.

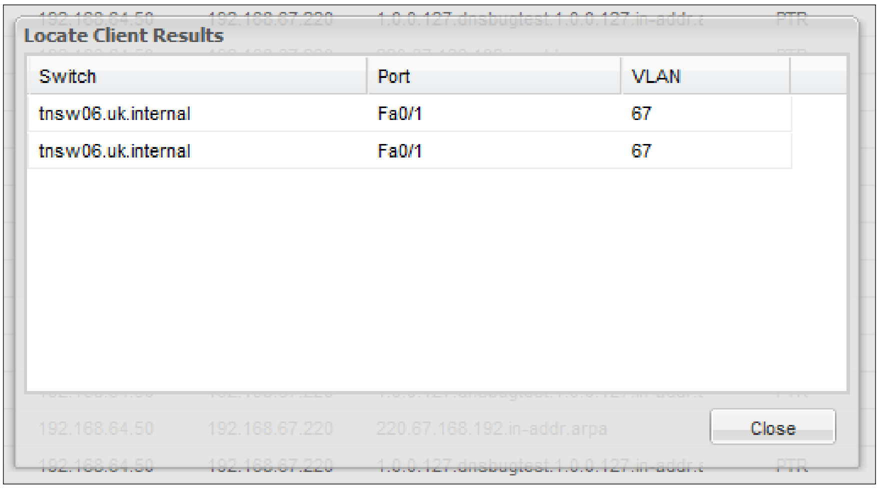
This feature is only available after the client location feature has been enabled. With this feature enabled, a right click menu is available within the DNS and DHCP activity logs, as demonstrated in the following examples.

In this first example, a DNS client is being located by its IP address by using the right-click menu:



	Client IP	Query Name
.50	192.168.67	ddr.arpa
.50	192.168.67	st.1.0.0.127.
.50	192.168.67.220	220.67.168.192.in-addr.arpa
.50	192.168.67.220	1.0.0.127.dnsbugtest.1.0.0.127.

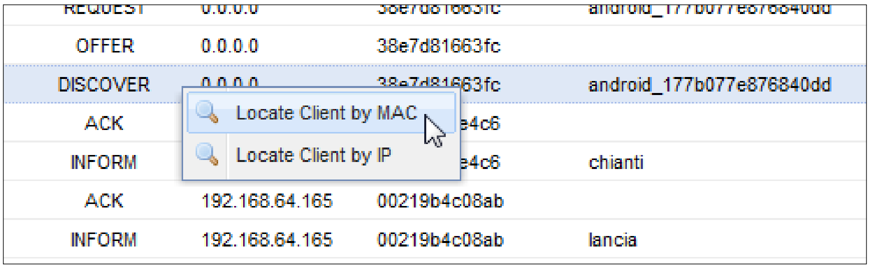
The resultant screen shows the output that was returned from porttracker/PortIQ, listing the switch, switch port and VLAN that the client is connected to. In cases where a client is misbehaving (e.g. virus infected and generating huge amounts of DNS query traffic) this feature could prove extremely useful as the DNS administrator can inform the network administrator exactly which switch and port the traffic is originating from so it can be shut down if required:



Locate Client Results

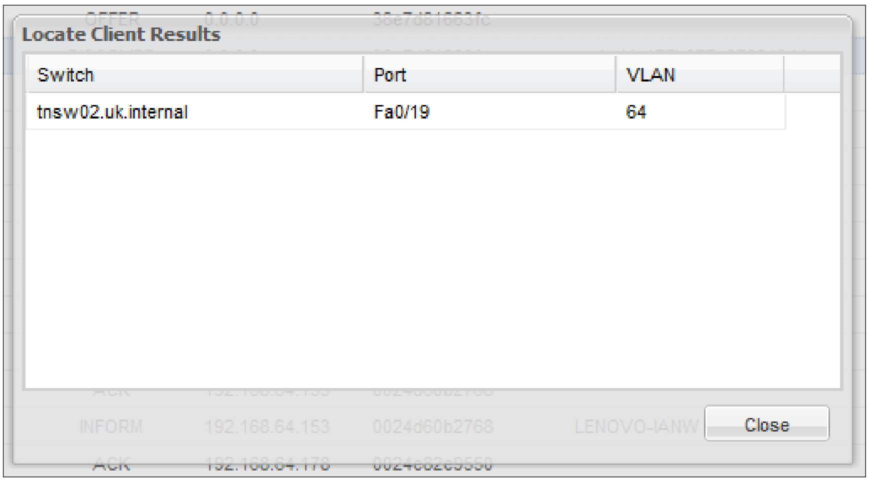
Switch	Port	VLAN
tnsw06.uk.internal	Fa0/1	67
tnsw06.uk.internal	Fa0/1	67

In this second example, a DHCP client is being located via its MAC address. In this particular case, the DHCP message is a DHCP DISCOVER, hence the client does not have an IP address yet (it could be located via its IP address if the client had completed the full DHCP lease acquisition process):



OFFER	0.0.0.0	38e7d81663fc	
DISCOVER	0.0.0.0	38e7d81663fc	android_177b077e876840dd
ACK		e4c6	
INFORM		e4c6	chianti
ACK	192.168.64.165	00219b4c08ab	
INFORM	192.168.64.165	00219b4c08ab	lancia

The resultant screen displays the information returned from porttracker/PortIQ with the switch name, port and VLAN information. Once again, this information could prove useful if a client is generating an abnormal amount of DHCP traffic:



Locate Client Results

Switch	Port	VLAN
tnsw02.uk.internal	Fa0/19	64

Refer to section 8.6 for more information on the client location feature and how it can be configured and enabled.

Chapter 6

6 Alerting

The Alert feature is accessed by clicking the "Alert" icon at the top right of the user interface:

NOTE: If the appropriate permissions have not been given this icon will not be displayed.

DDAM can be configured to alert when monitored activity matches a specific condition. Alerts are generated in real-time on Collectors.

An alerting process on each collector then dispatches alerts using one or more Alerting Methods (for example SNMP traps).

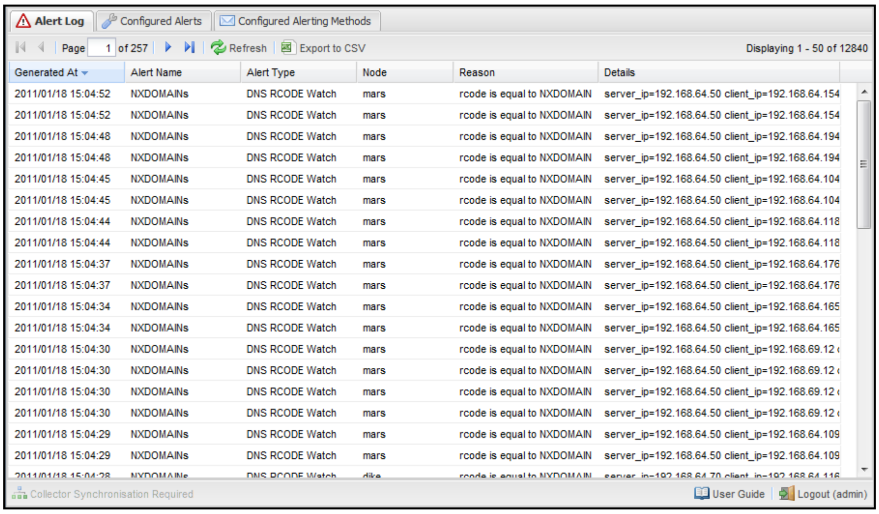
Generated alerts are written to an alert log on each collector. The alert log is periodically downloaded from each collector and cleared.

Alerts are appended to alert log files found under the "<install>/master/alerts" directory. A file will exists under this directory for each Node defined in DDAM.

The system will maintain the previous 10,000 alerts generated on a per Node basis.

6.1 Alert Log

Upon navigation to the Alerts page the "Alert Log" tab is displayed by default:


Alert Log
Configured Alerts
Configured Alerting Methods
Page 1 of 257
Refresh
Export to CSV
Displaying 1 - 50 of 12840
Collector Synchronisation Required
User Guide
Logout (admin)

Generated At	Alert Name	Alert Type	Node	Reason	Details
2011/01/18 15:04:52	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.154
2011/01/18 15:04:52	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.154
2011/01/18 15:04:48	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.194
2011/01/18 15:04:48	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.194
2011/01/18 15:04:45	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.104
2011/01/18 15:04:45	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.104
2011/01/18 15:04:44	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.118
2011/01/18 15:04:44	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.118
2011/01/18 15:04:37	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.176
2011/01/18 15:04:37	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.176
2011/01/18 15:04:34	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.165
2011/01/18 15:04:34	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.165
2011/01/18 15:04:30	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.69.12
2011/01/18 15:04:30	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.69.12
2011/01/18 15:04:30	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.69.12
2011/01/18 15:04:30	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.69.12
2011/01/18 15:04:29	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.109
2011/01/18 15:04:29	NXDOMAINs	DNS RCODE Watch	mars	rcode is equal to NXDOMAIN	server_ip=192.168.64.50 client_ip=192.168.64.109
2011/01/18 15:04:28	NXDOMAINs	DNS RCODE Watch	dike	rcode is equal to NXDOMAIN	server_ip=192.168.64.70 client_ip=192.168.64.116

The "Alert Log" tab displays alerts that have been generated across all Nodes. Filters can be used to interrogate the Alert Log, and filtered data can be exported.

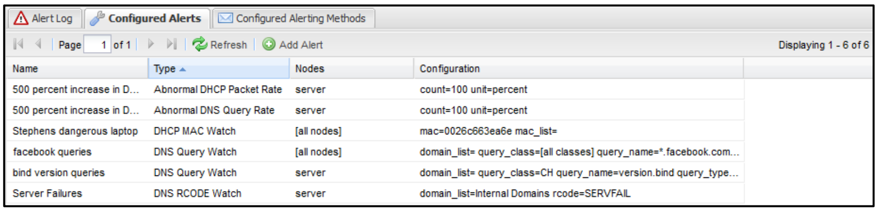
The following columns are displayed in this view:

Column	Filter Type	Description
Generated At	Date/Time	Date and time the alert was generated.
Alert Name	String	Name given to the alert when it was added.
Alert Type	N/A	The type of alert - see the Available Alert Types section below for a list of possible alerts.
Node	String	Name of the Node the alert was generated for.
Reason	String	A summary of why the alert was generated.
Details	String	A list of key/value pairs giving details about the parameters that

		generated the alert.

6.2 Configured Alerts

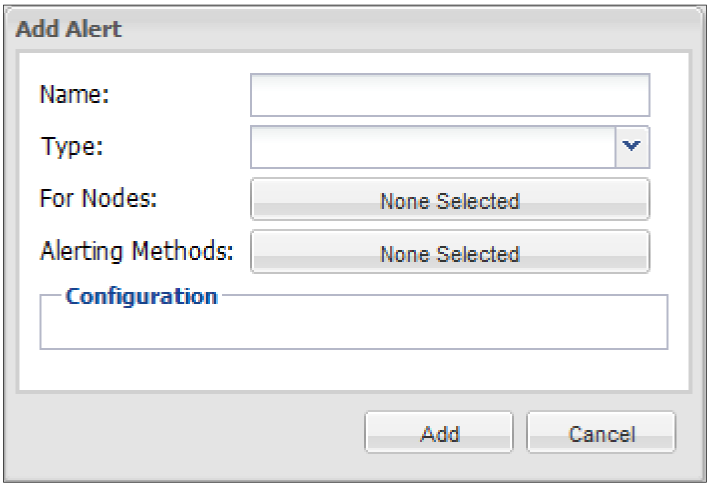
Under the Configured Alerts tab, the type of activity that triggers an alert can be managed. Alerts can be configured on a per node basis, or across all Nodes.



Name	Type	Nodes	Configuration
500 percent increase in D...	Abnormal DHCP Packet Rate	server	count=100 unit=percent
500 percent increase in D...	Abnormal DNS Query Rate	server	count=100 unit=percent
Stephens dangerous laptop	DHCP MAC Watch	[all nodes]	mac=0026c663ea6e mac_list=
facebook queries	DNS Query Watch	[all nodes]	domain_list= query_class=[all classes] query_name=*.facebook.com...
bind version queries	DNS Query Watch	server	domain_list= query_class=CH query_name=version.bind query_type...
Server Failures	DNS RCODE Watch	server	domain_list=Internal Domains rcode=SERVFAIL

After adding or modifying an alert, it is necessary to perform a collector synchronization in order to "push" the new alert configuration out to the relevant collector. A collector synchronization pop-up will alert you to this fact.

To add an alert click the "Add Alert" button in the toolbar, after which the "Add Alert" dialog will be displayed.

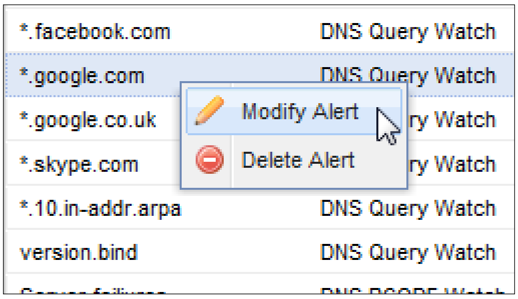


The following table describes each field displayed:

Field	Description
Name	A descriptive name for the alert. This can be used to identify this alert in emails, SNMP traps and the Alert Log.

Type	The type of alert to add. Refer to the Available Alerts section below for more details on the types of alerts available and their configurable parameters.
For Nodes	Use this button to select which Nodes the alert should be configured for.
Alerting Methods	Use this button to select which alerting methods should be used to dispatch alerts from collectors. If no alerting methods have been configured yet none can be selected. If no alerting method is selected, alerts will still be displayed in the "Alert Log" tab, but no alert (e.g. via SMTP or SNMP) will be generated. It may be desirable to configure some types of alerts with no alerting method configured so as to avoid swamping the alert destination with repetitive alerts (no alert normalization or consolidation is performed by DDAM so a busy system could potentially generate a large number of alerts, dependent upon the alert configuration).
Configuration	Upon selecting an alert type from the "Type" dropdown box this area will be populated with configuration fields relevant to the alert type. Refer to the Available Alerts section below for more details on the types of alerts available and their configurable parameters.

Alerts can be modified or deleted simply by right-clicking and selecting "Modify Alert" or "Delete Alert" from within the list of configured alerts.



*.facebook.com	DNS Query Watch
*.google.com	DNS Query Watch
*.google.co.uk	ry Watch
*.skype.com	ry Watch
*.10.in-addr.arpa	DNS Query Watch
version.bind	DNS Query Watch

The following sections detail the types of alerts currently available.

6.2.1 Abnormal DHCP Packet Rate

This alert detects variations in DHCP packet rate against a baseline. The baseline is created over a period of time. Thresholds can be specified as a percentage or a count against the baseline.

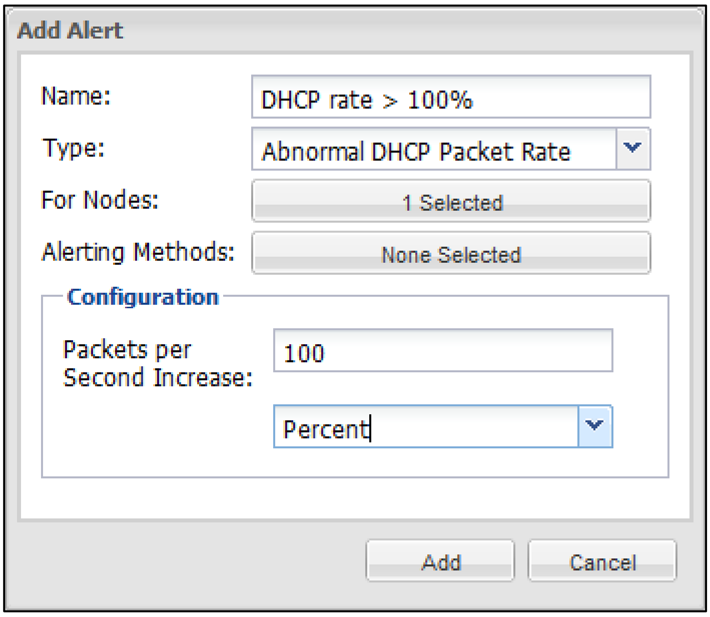
The following configurable options are available for this alert:

Option	Description
Packets per Second Increase	By how many "Units" should the packet rate increase above the calculated baseline to trigger this alert.
Unit	Whether a rate increase should be calculated as a percentage, count of packets or an absolute maximum throughput limit.

This alert is calculated every second. When the packet rate moves above the calculated threshold, one alert is generated. When the packet rate moves back down below the calculated threshold another alert is generated indicating so.

This prevents many alerts from being generated for every second the packet rate is above the calculated threshold.

In the following example, an Abnormal DHCP Packet Rate alert is being defined that will generate an alert if the DHCP packet rate increases above 100% of the currently calculated baseline at that point in time. This will enable an operator to be immediately notified if abnormal DHCP activity is detected:



Add Alert

Name: DHCP rate > 100%

Type: Abnormal DHCP Packet Rate

For Nodes: 1 Selected

Alerting Methods: None Selected

Configuration

Packets per Second Increase: 100

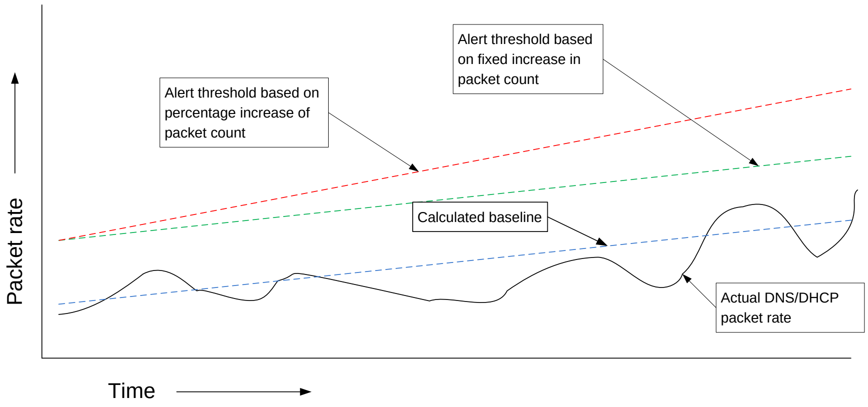
Percent

6.2.1.1 Percentage vs Packets

Using a rate increase that is based upon packets locks the threshold at a certain number of packets above the baseline regardless of the value of the baseline.

Using a rate increase that is based upon a percentage means that the threshold will increase as the baseline increases, therefore a greater number of packets will be required to trigger an alert if the baseline packet rate is higher.

The following diagram illustrates the difference between the two options:

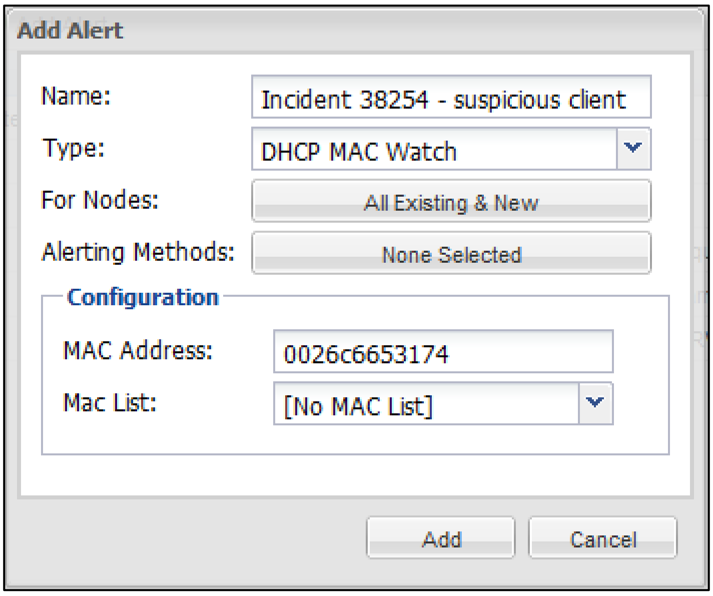


6.2.2 DHCP MAC Watch

This alert detects specific chaddr (Client Hardware Address) values in DHCP packets. One can exactly match a MAC address, or match the beginning or end by using the wildcard character (e.g. 045453*, which is one of the prefixes belonging to Apple Inc.).

A predefined MAC List can also be specified. Refer to section 4.8 for more information on MAC lists.

In the following example, a DHCP MAC Watch alert is being defined that will generate an alert if a specific MAC address is seen by a DHCP server:



Add Alert

Name: Incident 38254 - suspicious client

Type: DHCP MAC Watch

For Nodes: All Existing & New

Alerting Methods: None Selected

Configuration

MAC Address: 0026c6653174

Mac List: [No MAC List]

6.2.3 *Abnormal DNS Query Rate*

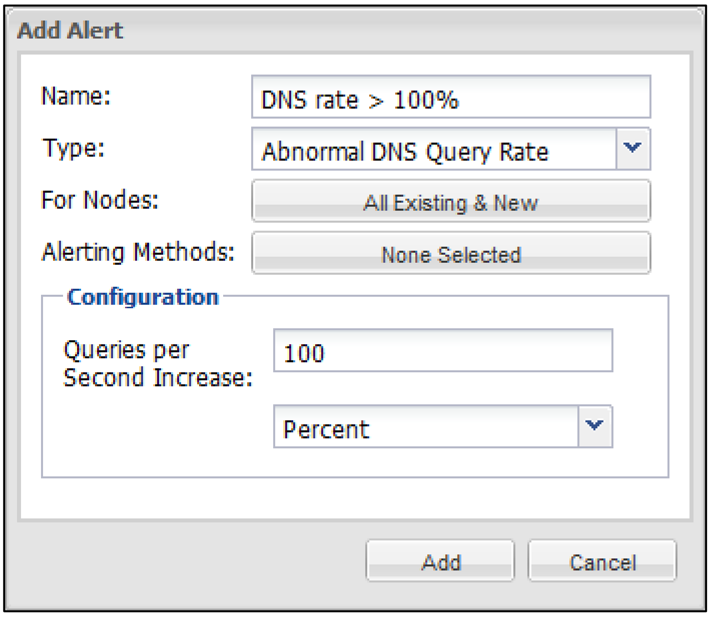
This alert detects variations in DNS query rate against a baseline. The baseline is created over a period of time. Increase thresholds can be specified as a percentage or a count against the baseline.

The following configurable options are available for this alert:

Option	Description
Queries per Second Increase	By how many "Units" should the query rate increase above the calculated baseline to trigger this alert.
Unit	Whether a rate increase should be calculated as a percentage, count of queries or an absolute maximum throughput limit.

This alert is calculated every second. When the query rate moves above the calculated threshold one alert is generated. When the packet rate moves back down below the calculated threshold another alert is generated indicating so.

This prevents many alerts from being generated for every second the query rate is above the calculated threshold.



Add Alert

Name: DNS rate > 100%

Type: Abnormal DNS Query Rate

For Nodes: All Existing & New

Alerting Methods: None Selected

Configuration

Queries per Second Increase: 100

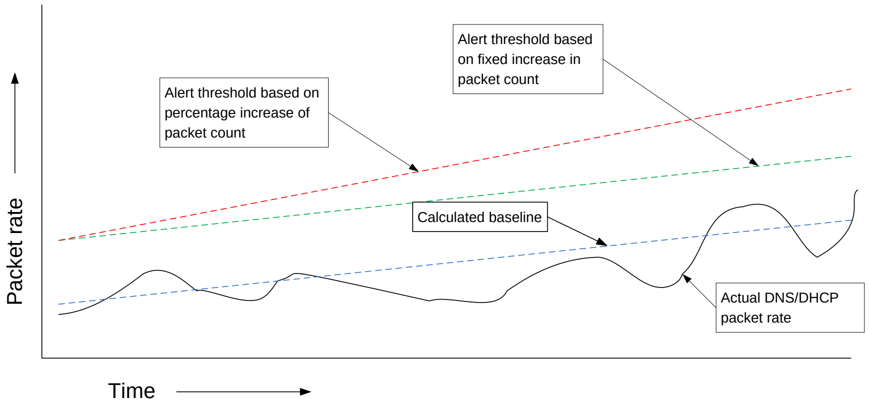
Percent

6.2.3.1 Percentage vs Packets

Using a rate increase that is based upon packets locks the threshold at a certain number of packets above the baseline regardless of the value of the baseline.

Using a rate increase that is based upon a percentage means that the threshold will increase as the baseline increases, therefore a greater number of packets will be required to trigger an alert if the baseline packet rate is higher.

The following diagram illustrates the difference between the two options:

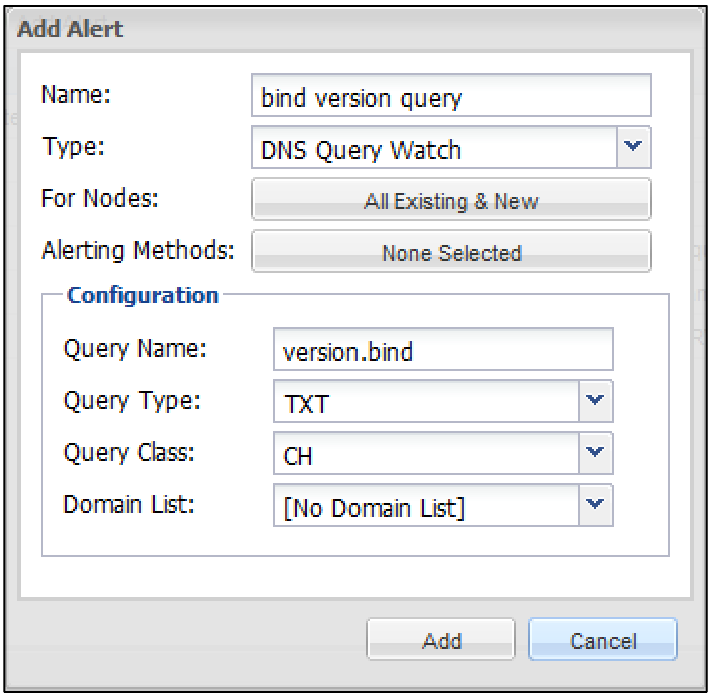


6.2.4 DNS Query Watch

This alert detects specific query name, type and classes in DNS queries. This alert can be configured to exactly match a query name, match the beginning or match the end (e.g. by using wildcards such as “*.ru”), optionally all query class and types can be matched or only specific ones.

Multiple query names can be specified by utilizing a Domain List (e.g. to generate an alert when a query for a malicious domain is detected). Refer to section 4.7 for more information on domain lists.

In the following example, a DNS Query Watch alert is being defined that will generate an alert if any queries for "version.bind" of type TXT and class CHAOS are detected. This query is normally used by a malicious user who is attempting to "fingerprint" the type of DNS server that is being used; hence it is useful to be alerted to these types of queries:



Name: bind version query

Type: DNS Query Watch

For Nodes: All Existing & New

Alerting Methods: None Selected

Configuration

Query Name: version.bind

Query Type: TXT

Query Class: CH

Domain List: [No Domain List]

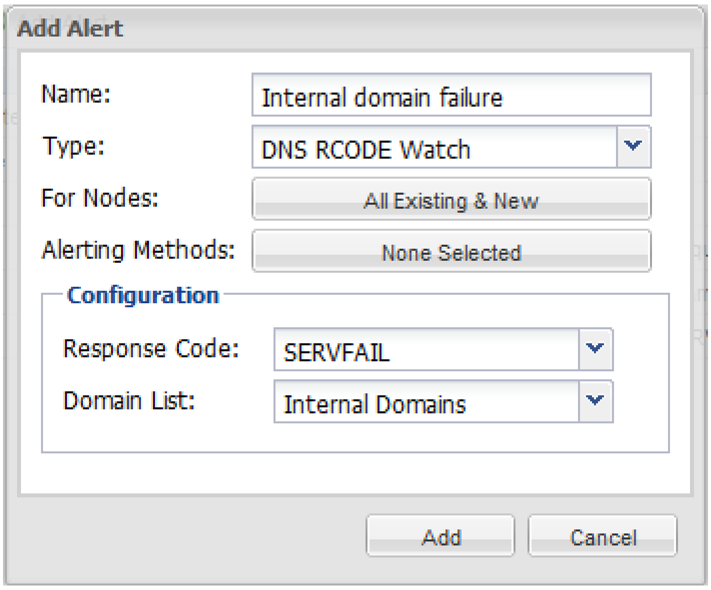
To specify a Domain List, simply select it from the "Domain Lists" drop down.

6.2.5 DNS RCODE Watch

This alert detects responses that resulted in a specific response code.

A predefined Domain List can also be specified so that alerts are only generated for specific domains (rather than everything). Refer to section 4.7 for more information on Domain Lists.

In the following example, a DNS RCODE Watch alert is being defined that will generate an alert if any responses with a response code of "SERVFAIL" are detected for any domain defined in the “Internal Domains” domain list:



Name: Internal domain failure

Type: DNS RCODE Watch

For Nodes: All Existing & New

Alerting Methods: None Selected

Configuration

Response Code: SERVFAIL

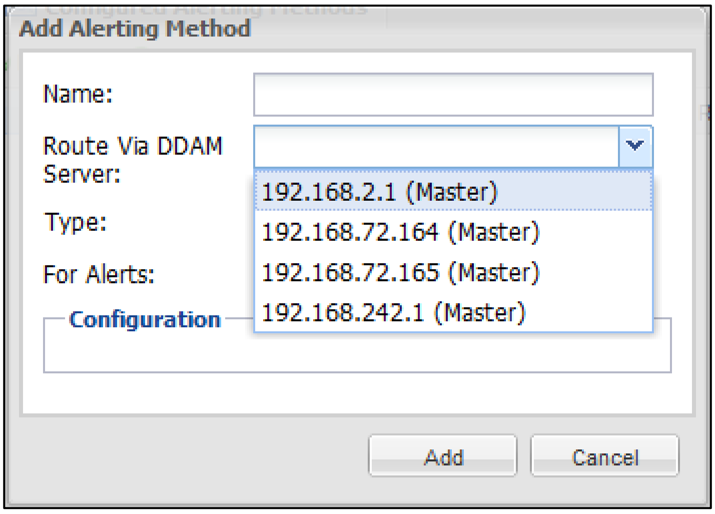
Domain List: Internal Domains

6.3 Configure Alerting Methods

Under the "Configure Alerting Methods" tab, the type of alerts that should be dispatched from DDAM can be managed.

By default alerts are dispatched directly from the Collector on which the alert was generated. The DDAM server from which alerts can be dispatched can be specified when configuring alerting methods.

Alerts can be dispatched from any server in a DDAM installation, regardless of where it was originally generated, by specifying the server in “Route via DDAM Server” dropdown box:

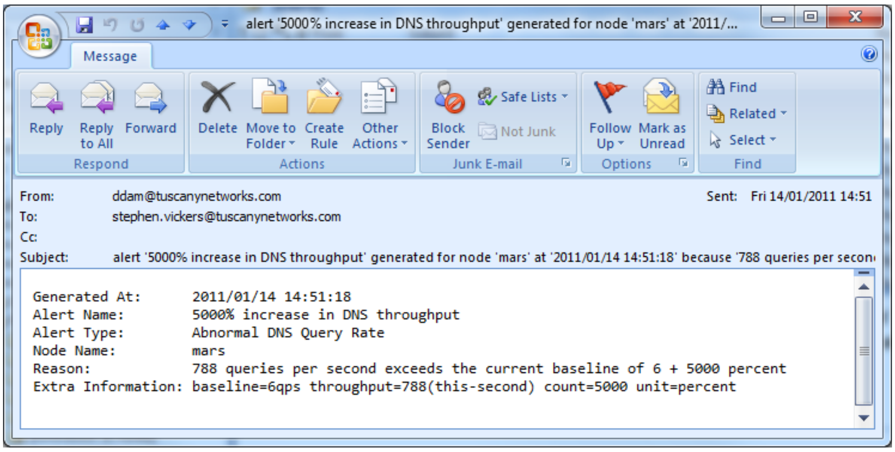


NOTE: A firewall rule allowing TCP traffic from the Collector on which the alert was generated to port 60001 on the selected server should be in place for alerts to be dispatched successfully.

6.3.1 SMTP Mail

Configuring this alerting method and associating alerts with it causes generated instances of the alerts to be dispatched via SMTP mail from Collectors.

The following is an example SMTP alert from a DDAM Collector:



From: ddam@tuscanynetworks.com
Sent: Fri 14/01/2011 14:51
To: stephen.vickers@tuscanynetworks.com
Cc:
Subject: alert '5000% increase in DNS throughput' generated for node 'mars' at '2011/01/14 14:51:18' because '788 queries per secon

```
Generated At:      2011/01/14 14:51:18
Alert Name:        5000% increase in DNS throughput
Alert Type:        Abnormal DNS Query Rate
Node Name:         mars
Reason:            788 queries per second exceeds the current baseline of 6 + 5000 percent
Extra Information: baseline=6qps throughput=788(this-second) count=5000 unit=percent
```

Each email will detail what alert has been generated, at what time and why.

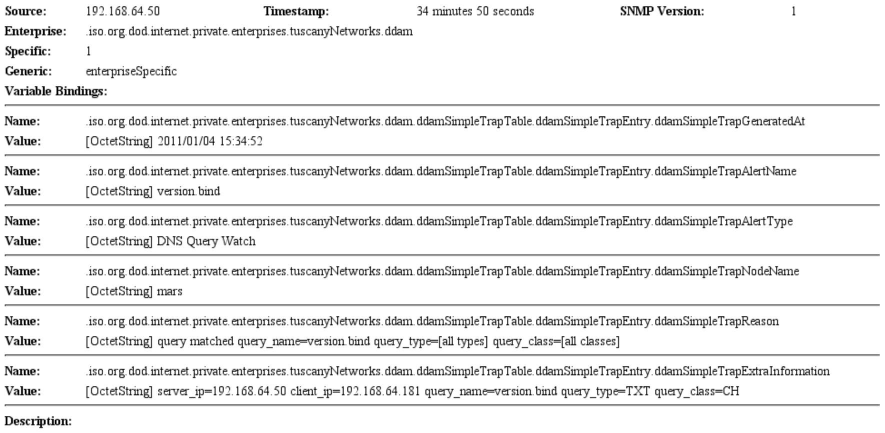
The following configurable options are available for this alerting method:

Option	Description
From Email	Email address SMTP mail alerts should appear to be from.
To Email	A comma separated list of email addresses alerts should be sent to.
SMTP Server	IP address or hostname of SMTP server.
SMTP Port	SMTP server port number.

6.3.2 SNMP Version 1 Trap

Configuring this alerting method and associating alerts with it causes generated instances of the alerts to be dispatched via SNMP from Collectors to an SNMP trap receiver.

The following is an example SNMP alert from a DDAM Collector:



```
Source:      192.168.64.50          Timestamp:      34 minutes 50 seconds          SNMP Version:      1
Enterprise:  .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam
Specific:    1
Generic:     enterpriseSpecific
Variable Bindings:
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapGeneratedAt
Value:       [OctetString] 2011/01/04 15:34:52
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapAlertName
Value:       [OctetString] version.bind
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapAlertType
Value:       [OctetString] DNS Query Watch
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapNodeName
Value:       [OctetString] mars
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapReason
Value:       [OctetString] query matched query_name=version.bind query_type=[all types] query_class=[all classes]
--------------------------------------------------------------------------------------------------------------
Name:        .iso.org.dod.internet.private.enterprises.tuscanyNetworks.ddam.ddamSimpleTrapTable.ddamSimpleTrapEntry.ddamSimpleTrapExtraInformation
Value:       [OctetString] server_ip=192.168.64.50 client_ip=192.168.64.181 query_name=version.bind query_type=TXT query_class=CH
--------------------------------------------------------------------------------------------------------------
Description:
```

The DDAM SNMP MIB can also be downloaded directly from the DDAM Master Server by using the following URL: https://<DDAM Master Server name or IP address>/doc/DDAM-MIB.txt

Refer to the DDAM-MIB.txt file, which can be located in the "<install>/www/doc" directory on the DDAM master server, for more information on what's contained in an SNMP trap.

The following configurable options are available for this alerting method:

Option	Description
Trap Server	IP address or hostname of the SNMP trap server.
Port	SNMP trap server port.
Community	SNMP community string

6.3.3 Execute Command

Configuring this alerting method and associating alerts with it causes generated instances of the alerts to be passed to a specified command.

The command specified must be installed on the appropriate collectors, or the DDAM server specified in the “Route via DDAM Server” option.

The command specified will be invoked for each generated alert.

Once invoked the following information will be passed to the commands standard input as key/value pairs separated by a ":" on separate lines:

- Generated At – when the alert was generated, e.g. “2012/01/23 09:41:10”
- Alert Name - name of the alert as defined in the product
- Alert Type - type of the alert, as selected when adding the alert, e.g. “DNS Query Watch”
- Node Name - name of the node the alert was generated for

- Reason - short text string describing why the alert was generated
- Extra Information - per alert information, such as client_ip or query_name

After all key/value pairs have been printed to the commands standard input the line "End Alert" will printed to indicate no more key/value pairs will occur and the alert can be consumed.

The following is example text which will be printed to a commands standard input:

```
Generated At:2012/01/23 09:41:10
Alert Name:bad.uk.internal
Alert Type:DNS Query Watch
Node Name:mars
Reason:query matched query_name=bad.uk.internal
query_type=[all types] query_class=[all classes]
Extra Information:server_ip=192.168.64.50
client_ip=192.168.64.45 query_name=bad.uk.internal
query_type=A query_class=IN
End Alert
```

The following is an example Perl script which receives generated alerts:

```
#!/usr/bin/perl

my %alert;

while (<>) {
        last if /^end alert/i;
        my ($k, $v) = split /\:/, $_, 2;
        $alert{$k} = $v;
}

# do something with the alert...
```

Failures in a command are ignored. If a failure occurs alerts will NOT be kept and fed to the command again later. This prevents a backlog of alerts from building up.

The standard output and standard error of commands are ignored and will simply be redirected to the <install>/log/alertd.log file (or <install>/log/msgd.log if the "Route via DDAM Server" parameter has been specified).

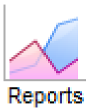
The following configurable options are available for this alerting method:

Option	Description
Command	Full path to the command.
Argument	Arguments to the command.

Chapter 7

7 Reporting

The reporting feature can be accessed by clicking the Report icon at the top of the page:



NOTE: If the appropriate permissions have not been given this icon will not be displayed.

PNG stands for "Portable Network Graphics" and is a file format commonly used today for producing compressed graphic images. It was designed to replace the earlier GIF file format that suffers from patent issues.

Under the reporting page, instantly generated chart based and tabular based reports can be viewed, or scheduled PDF reports can be managed along with report publishing methods.

NOTE: By default Adobe Flash Player is used to display chart based data. If flash is not detected the system will fall back to using PNG based charts. This can be controlled under the options menu when viewing charts. Flash based charts are preferable as they are generated much quicker and they enable the user to hover the mouse over a point on the graph and obtain a pop-up of the exact value at that point and. This feature is not available with PNG based charts.

Adobe Flash can be obtained from the following URL: http://get.adobe.com/flashplayer/

7.1 Periods & Resolutions

When viewing charts and tables, the data can be viewed for a certain period of time. The period might cover a specific hour, day, week, month or year.

In order to prevent huge amounts of data being stored by DDAM, the data within each period is only stored at a certain resolution. For example, when chart data is viewed for an hourly period, each data point on the chart represents one minute. However it is not possible to store every single minute of data for a whole year, so after a certain amount of time each minute is rolled up to an hourly resolution. After a longer period of time, the hours are rolled up into days and days are eventually rolled up into months.

For example, a chart could have a period set to "Hourly by Minute" -> "2010/10/01 09:00:00". This would cover the hour starting 09:00 on 1st October 2010 and provide a data point on the chart for each minute of that hour. The previous 24 hours can be viewed at this resolution. For older data, the resolution is reduced, for instance the period could be set to "Daily by Hour" -> "2010/09/30" to view the data for the previous day, but at an hourly resolution.

DDAM will store 24 hours worth of hourly periods at one minute resolution, after which it starts to roll the data up.

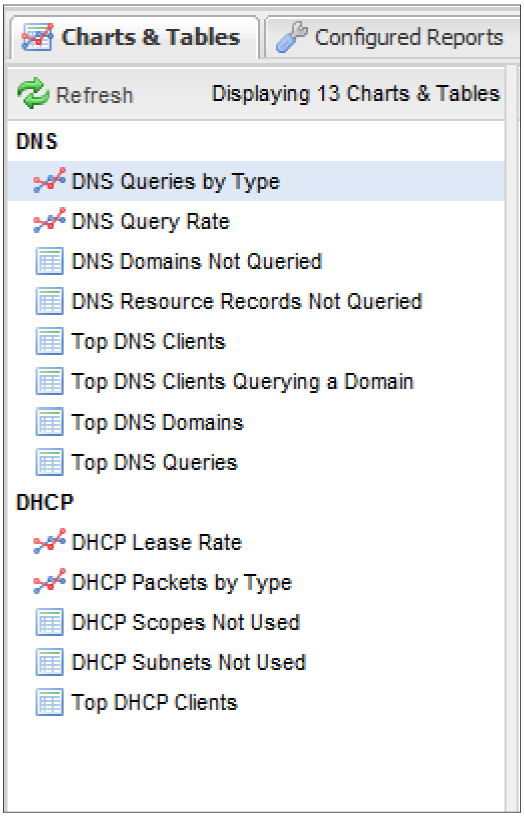
As time advances, the system will continue to roll data up for each period so as not to fill the disk on the master DDAM server.

The following resolutions are available for all charts and tables with the exception of the Not Used/Queried reports:

Period	Resolution (for charts)	Amount of data kept for each period
Hourly	By minute	24 hours
Daily	By hour	7 days
Weekly	By hour	8 weeks
Monthly	By day	12 months
Yearly	By month	All

7.2 Charts & Tables

Charts and tables can be viewed by clicking the "Charts & Tables" tab under the Reports page. A list of available charts and tables is found under this page to the left of the screen:



Displaying 13 Charts & Tables

DNS

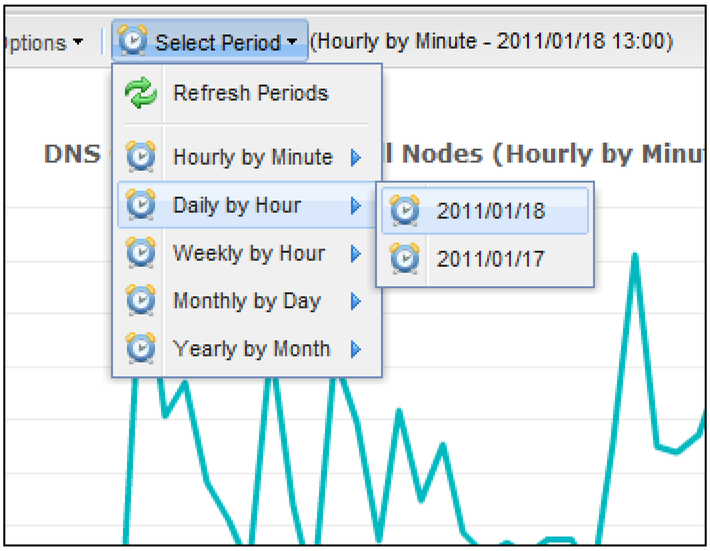
- DNS Queries by Type
- DNS Query Rate
- DNS Domains Not Queried
- DNS Resource Records Not Queried
- Top DNS Clients
- Top DNS Clients Querying a Domain
- Top DNS Domains
- Top DNS Queries

DHCP

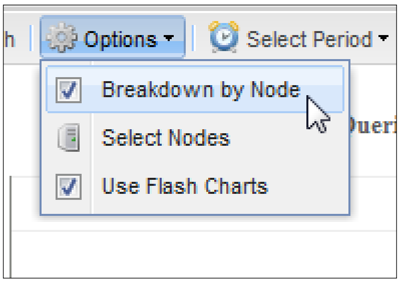
- DHCP Lease Rate
- DHCP Packets by Type
- DHCP Scopes Not Used
- DHCP Subnets Not Used
- Top DHCP Clients

To view data for a chart or table simply click the desired item.

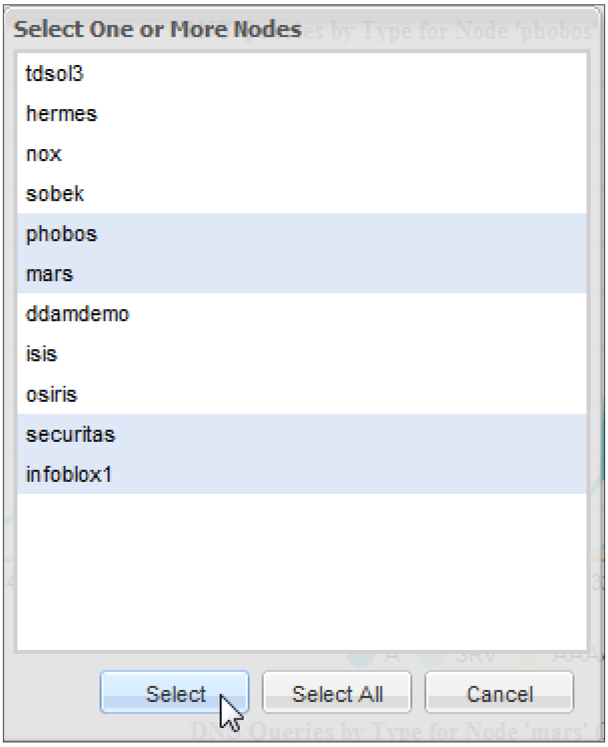
With the exception of the Not Used/Queried charts, once a chart or table has been selected, the period and resolution can be changed to view different time windows.



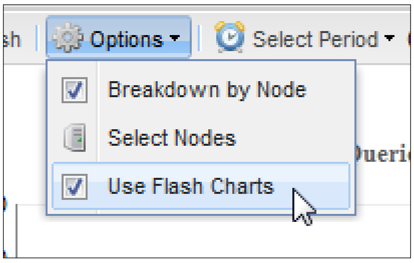
The reports summarize the data across all nodes by default. To see a breakdown of the data for each node, the "Breakdown by Node" option can be selected from the Options menu.



If data for only one node or specific nodes is required (rather than all), the "Select Nodes" option can be used to specify which nodes to report on:

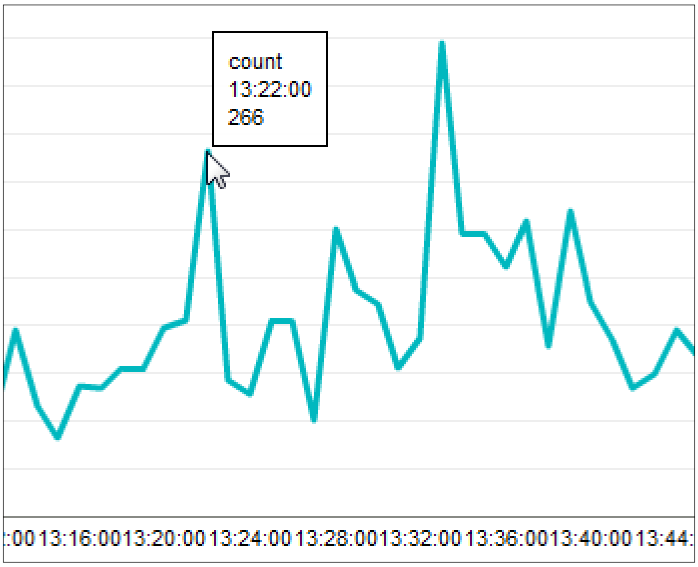


For charts, there is an option under the options menu to control whether Adobe Flash or a static PNG graphic is used to display graphical charts (NOTE: this option will be deselected and disabled if Adobe Flash Player is not installed):



Disabling Flash based charts (by unticking "Use Flash Charts") will cause charts to be rendered as a static PNG graphic and may be useful so that the chart can be "copied and pasted" into another document or email (i.e. by using the browsers right-click menu). Copy and paste isn't available with Flash based charts.

When Flash charts are enabled, data values can be displayed on the chart by hovering the mouse over a point on the chart. A pop-up will display the value at that point. In this example the pop-up is indicating a count of 266 DNS queries for the minute starting 13:22:

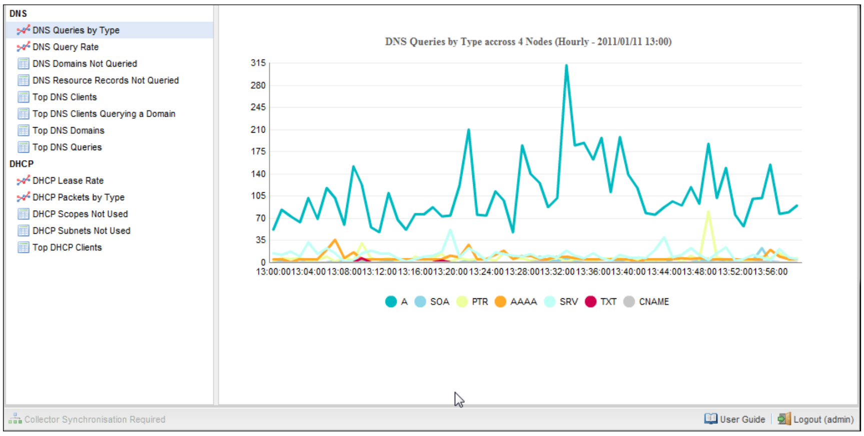


Flash based charts can be printed directly by right-clicking on the chart and using the "Print..." option. Reports can also be printed or exported as a PDF file – this is covered in section 7.3.

The following sections detail the reports that are currently available within DDAM.

7.2.1 DNS Queries by Type

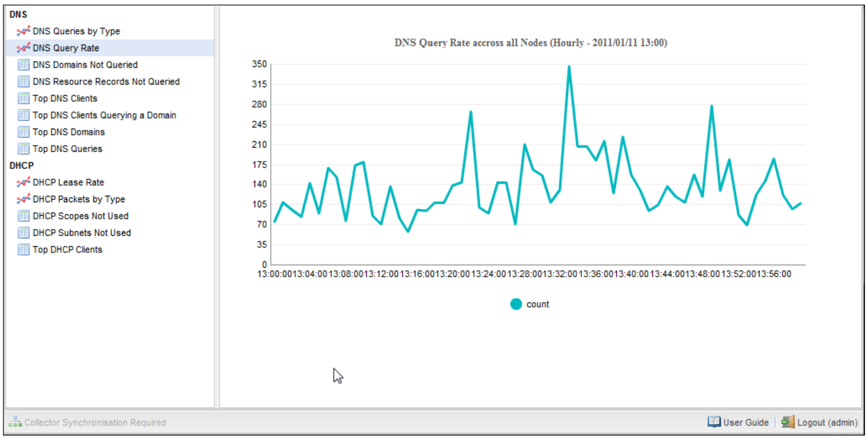
Total DNS query throughput by DNS resource record type per chart tick interval. A series will be plotted on the chart per DNS query type seen.



The chart tick interval will vary based on what resolution has been selected. See the Periods & Resolutions section for more information on chart tick intervals used for each available resolution.

7.2.2 DNS Query Rate

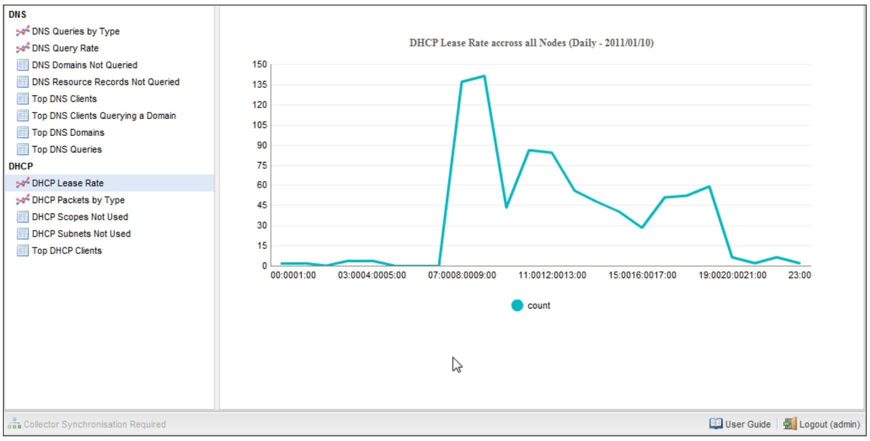
Total DNS query throughput per chart tick interval. A single series will be plotted on the chart.



The chart tick interval will vary based on what resolution has been selected. See the Periods & Resolutions section for more information on chart tick intervals used for each available resolution.

7.2.3 DHCP Lease Rate

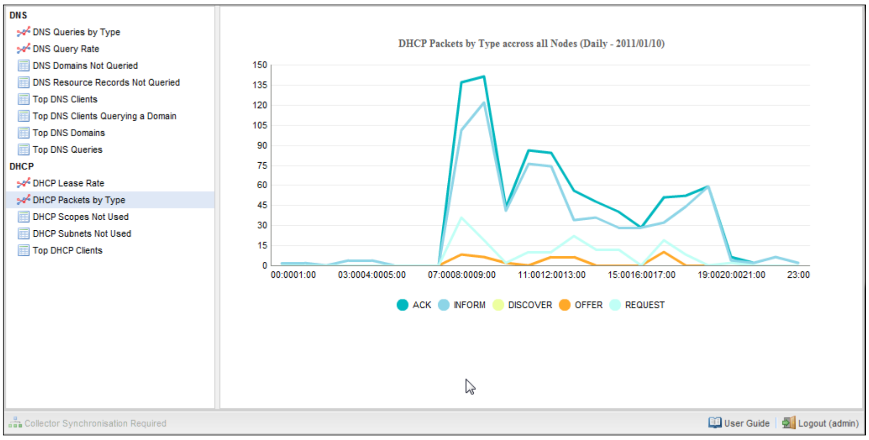
Total DHCP lease throughput per chart tick interval. A single series will be plotted on the chart.



The chart tick interval will vary based on what resolution has been selected. See the Periods & Resolutions section for more information on chart tick intervals used for each available resolution.

7.2.4 DHCP Packets by Type

Total DHCP packet throughput by DHCP message type per chart tick interval. A series will be plotted on the chart per DHCP message type seen.



The chart tick interval will vary based on what resolution has been selected. See the Periods & Resolutions section for more information on chart tick intervals used for each available resolution.

7.2.5 DNS Domains Not Queried

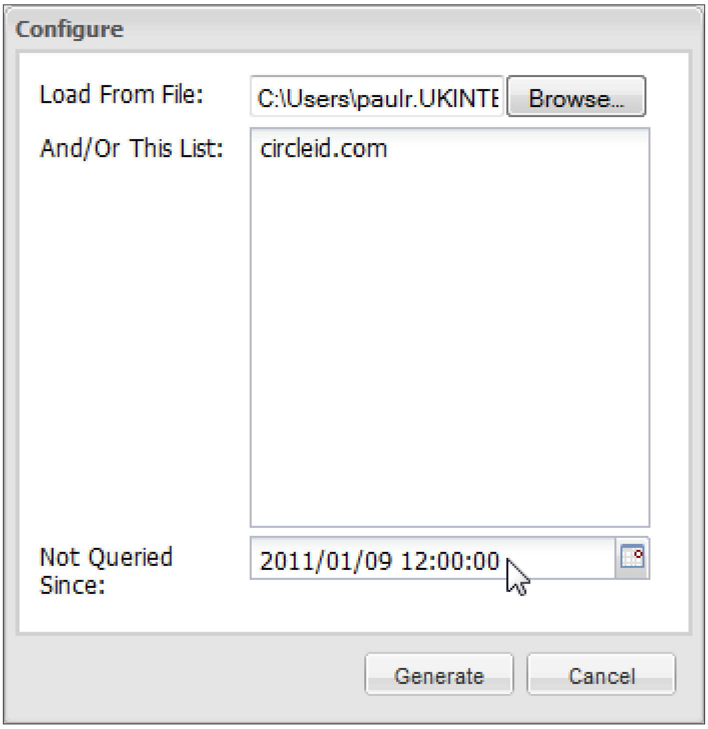
This report allows a list of domains for which no DNS queries have been seen for a period of time to be produced. The purpose of this report is to enable administrators, who have many domains defined on an authoritative DNS server, to identify which, if any, domains are not being queried. These domains could then become candidates for removal/reclamation.

NOTE: *The report is not restricted to just authoritative domains, but in fact can be used to check if any domains have or have not been queried since a particular date.*

In order to generate this report, the system needs to be configured with a list of domains that it should check.

When generating data for this report, a DNS domain list can be loaded from a text file or a named.conf configuration file from a BIND based DNS server can be used. A list of DNS domains can also be manually entered into a textbox (and will supplement any file that is loaded).

To generate a report click the "Regenerate" button, after which a Configure dialog will be displayed. The following options can be configured under this dialog:



Load From File: C:\Users\paulr.UKINTE

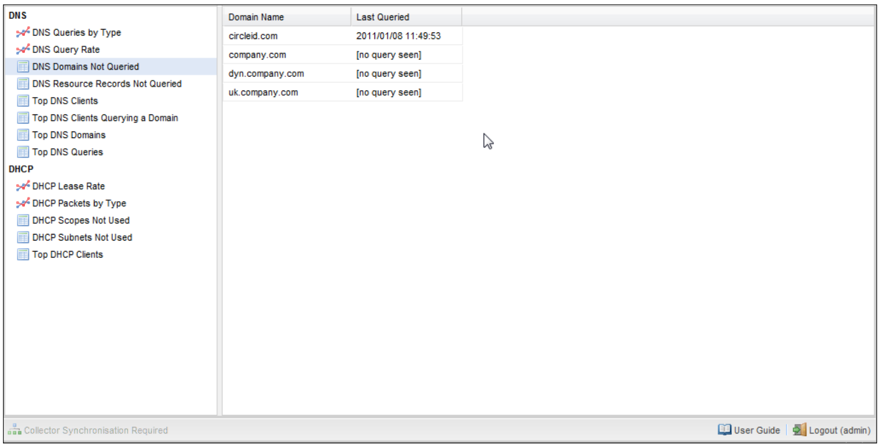
And/Or This List: circleid.com

Not Queried Since: 2011/01/09 12:00:00

Option	Description
Load From File	Specify a named.conf, from a Bind based DNS server, or a flat text file containing a list of DNS domains (one per line).
And/Or This List	A list of DNS domains (one per line).
Not Queried Since	Select the date/time after which a DNS query must not have been seen for a domain to be displayed in the generated report.

After the report has been configured, the "Generate" button can be clicked to generate the report.

The report will produce a list of DNS domains for which no query has been seen since the date specified in the configure dialog.



Domain Name	Last Queried
circleid.com	2011/01/08 11:49:53
company.com	[no query seen]
dyn.company.com	[no query seen]
uk.company.com	[no query seen]

The following columns are displayed:

Column	Description
Domain Name	Domain name.
Last Queried	If no query was ever seen for this DNS domain "[no query seen]" will be displayed in this column, otherwise the date of the last query under this domain will be displayed.

NOTE: If a domain is not listed, it is because it has been detected in a query since the "Last Queried" date.

7.2.6 DNS Resource Records Not Queried

This report allows a list of resource records for which no DNS queries have been seen for a period of time to be produced. The purpose of this report is to enable administrators to identify which resource records are not being queried. This may be useful for zone maintenance, whereby redundant records can be removed.

In order to generate this report, the system needs to be configured with a list of resource records that it should check.

When generating data for this report, a list of resource records can be loaded from a text file or a DNS zone file from a BIND based

DNS server. Resource records can also be manually entered into a text box to supplement any file that is loaded.

If a BIND based zone file is used, it must have a filename that conforms to the convention used in the O'Reilly DNS & BIND book, i.e. db.zonename, e.g. db.uk.internal.

NOTE: If a flat text file is used, each line must contain a fully qualified domain name and optionally the record type and class in comma separated format. Both of the following are acceptable:

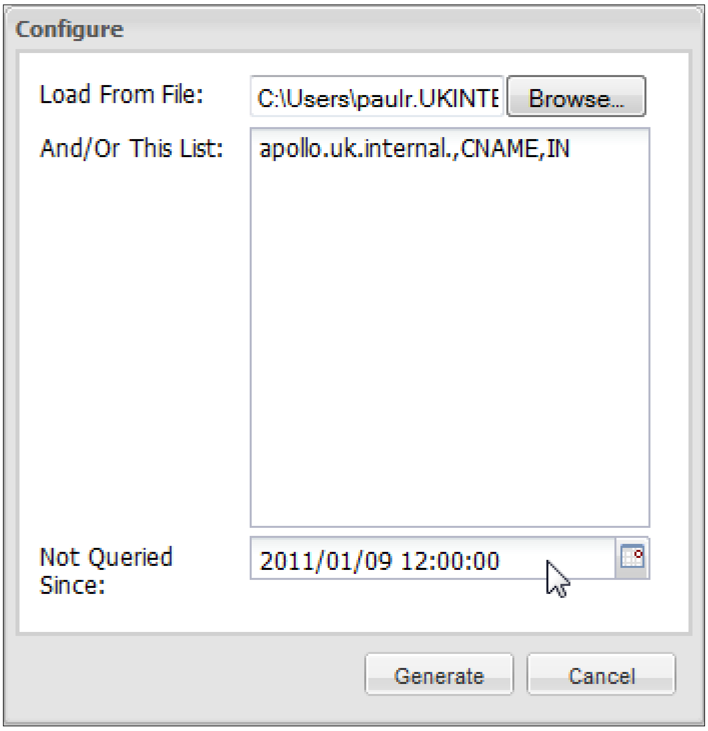
```
server1.uk.internal.
```

or:

```
server2.uk.internal.,CNAME,IN
```

Both record formats can be used if records are entered manually into the text box.

To generate a report click the "Regenerate" button, after which a Configure dialog will be displayed. The following options can be configured under this dialog:



Load From File: C:\Users\paulr.UKINTE

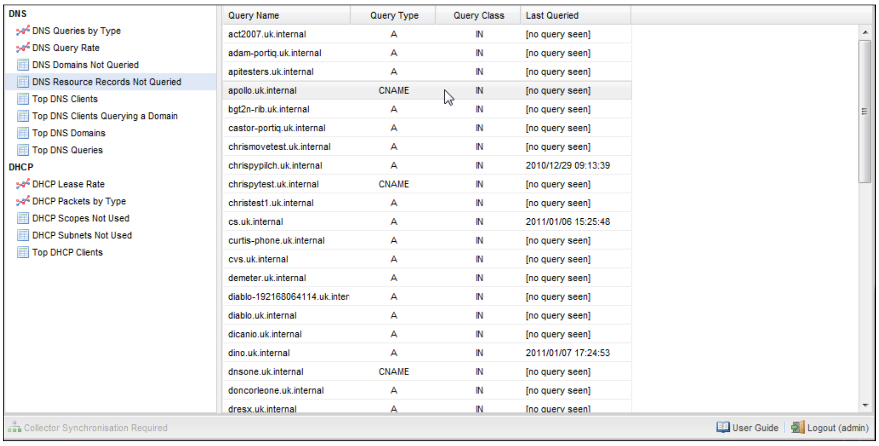
And/Or This List: apollo.uk.internal.,CNAME,IN

Not Queried Since: 2011/01/09 12:00:00

Option	Description
Load From File	Specify a DNS zone file, from a BIND based DNS server, or a flat text file containing a list of resource records.
And/Or This List	A list of resource records that supplements any file loaded.
Not Queried Since	Select the date after which a DNS query must not have been seen for a resource record to be displayed in the generated report.

After the report has been configured, the "Generate" button can be clicked to generate the report.

The report will produce a list of DNS resource records for which no query has been seen since the date specified in the configure dialog.



Query Name	Query Type	Query Class	Last Queried
act2007.uk.internal	A	IN	[no query seen]
adam-portiq.uk.internal	A	IN	[no query seen]
apitesters.uk.internal	A	IN	[no query seen]
apollo.uk.internal	CNAME	IN	[no query seen]
bgt2n-rib.uk.internal	A	IN	[no query seen]
castor-portiq.uk.internal	A	IN	[no query seen]
chrismovetest.uk.internal	A	IN	[no query seen]
chrispypilch.uk.internal	A	IN	2010/12/29 09:13:39
chrispytest.uk.internal	CNAME	IN	[no query seen]
christest1.uk.internal	A	IN	[no query seen]
cs.uk.internal	A	IN	2011/01/06 15:25:48
curtis-phone.uk.internal	A	IN	[no query seen]
cvs.uk.internal	A	IN	[no query seen]
demeter.uk.internal	A	IN	[no query seen]
diablo-192168064114.uk.inter	A	IN	[no query seen]
diablo.uk.internal	A	IN	[no query seen]
dicanio.uk.internal	A	IN	[no query seen]
dino.uk.internal	A	IN	2011/01/07 17:24:53
dnsone.uk.internal	CNAME	IN	[no query seen]
doncorleone.uk.internal	A	IN	[no query seen]
dresx.uk.internal	A	IN	[no query seen]

The following columns are displayed:

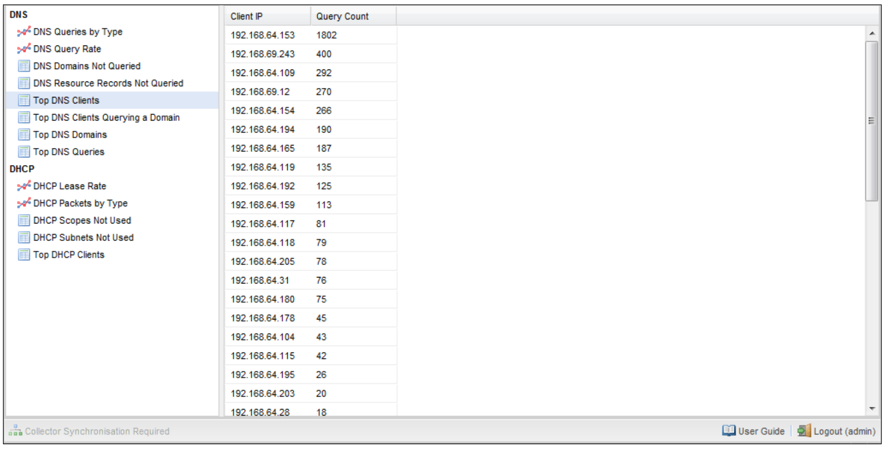
Column	Description
Query Name	Query name.

Query Type	If a DNS query type was specified in the flat text file, BIND zone file or text box, the report will display the query type, otherwise displays "[any type]" and the entry pertains to all query types.
Query Class	If a DNS query class was specified in the flat text file, BIND zone file or text box, the report will display the query class, otherwise displays "[any class]" and the entry pertains to all query classes.
Last Queried	If no query was ever seen for this resource record "[no query seen]" will be displayed in this column, otherwise the date of the last query for the resource record will be displayed.

NOTE: If a particular resource record is not listed in the report, it is because a query (or multiple queries) has been detected for that record since the "Last Queried" date.

7.2.7 Top DNS Clients

Displays a list of all DNS clients a query has originated from and the number of queries seen for each client. The table is ordered by count, highest first.



Client IP	Query Count
192.168.64.153	1802
192.168.69.243	400
192.168.64.109	292
192.168.69.12	270
192.168.64.154	266
192.168.64.194	190
192.168.64.165	187
192.168.64.119	135
192.168.64.192	125
192.168.64.159	113
192.168.64.117	81
192.168.64.118	79
192.168.64.205	78
192.168.64.31	76
192.168.64.180	75
192.168.64.178	45
192.168.64.104	43
192.168.64.115	42
192.168.64.195	26
192.168.64.203	20
192.168.64.28	18

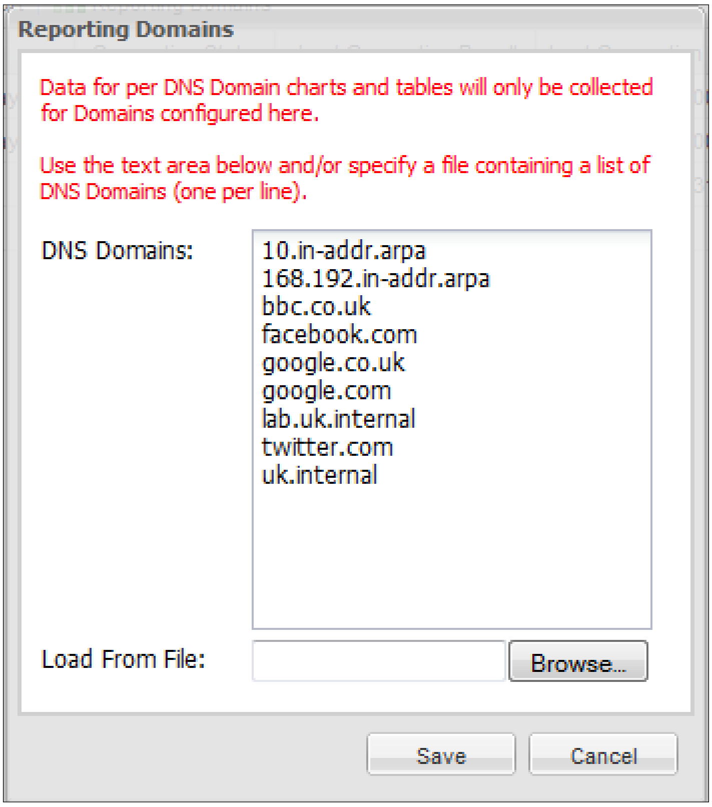
The following columns are available in this report:

Column	Filter Type	Description
Node	N/A	Node on which the data was seen. This column is only displayed if the "Breakdown by Node" checkbox is checked under the options menu.
Client IP	IP Address	IP address of the DNS client
Query Count	Number	Number of queries seen from the client for the period and resolution selected.

7.2.8 Top DNS Clients Querying a Domain

Displays a list of all DNS clients a query has originated from and the number of queries seen for each client on a per DNS domain basis. The table is ordered by count, highest first.

When processing fully qualified domain names, it is very difficult to establish which portion of the name actually represents the domain name (this is due to the wide scale use of "dotted hostnames"). Therefore in order to provide a report of "Top clients querying a domain", DDAM has to be configured with a list of domains that it can report against. These domains are called "Reporting Domains" and can be configured by selecting the "Reporting Domains" button on the "Configured Reports" tab:



Data for per DNS Domain charts and tables will only be collected for Domains configured here.

Use the text area below and/or specify a file containing a list of DNS Domains (one per line).

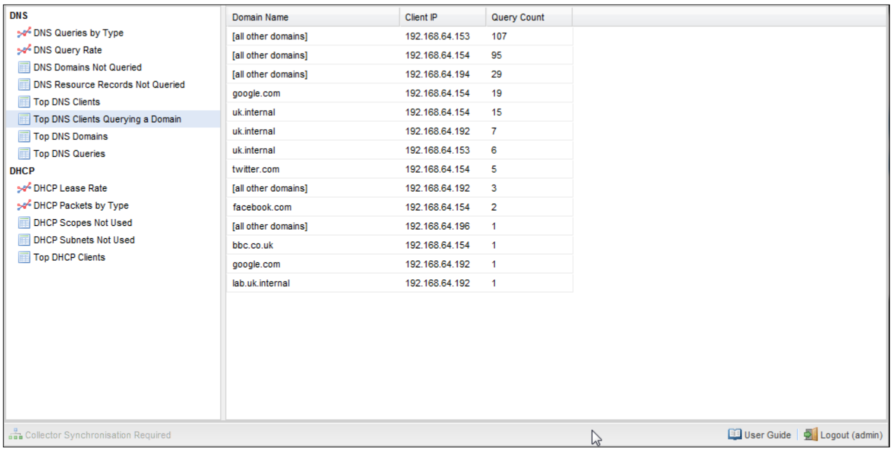
DNS Domains:

```
10.in-addr.arpa
168.192.in-addr.arpa
bbc.co.uk
facebook.com
google.co.uk
google.com
lab.uk.internal
twitter.com
uk.internal
```

Load From File:

The domain names listed in this report will depend on what reporting domains have been configured.

All queries not matching a domain defined as a reporting domain will be totaled under the domain "[all other domains]".



Domain Name	Client IP	Query Count
[all other domains]	192.168.64.153	107
[all other domains]	192.168.64.154	95
[all other domains]	192.168.64.194	29
google.com	192.168.64.154	19
uk.internal	192.168.64.154	15
uk.internal	192.168.64.192	7
uk.internal	192.168.64.153	6
twitter.com	192.168.64.154	5
[all other domains]	192.168.64.192	3
facebook.com	192.168.64.154	2
[all other domains]	192.168.64.196	1
bbc.co.uk	192.168.64.154	1
google.com	192.168.64.192	1
lab.uk.internal	192.168.64.192	1

The following columns are available in this report:

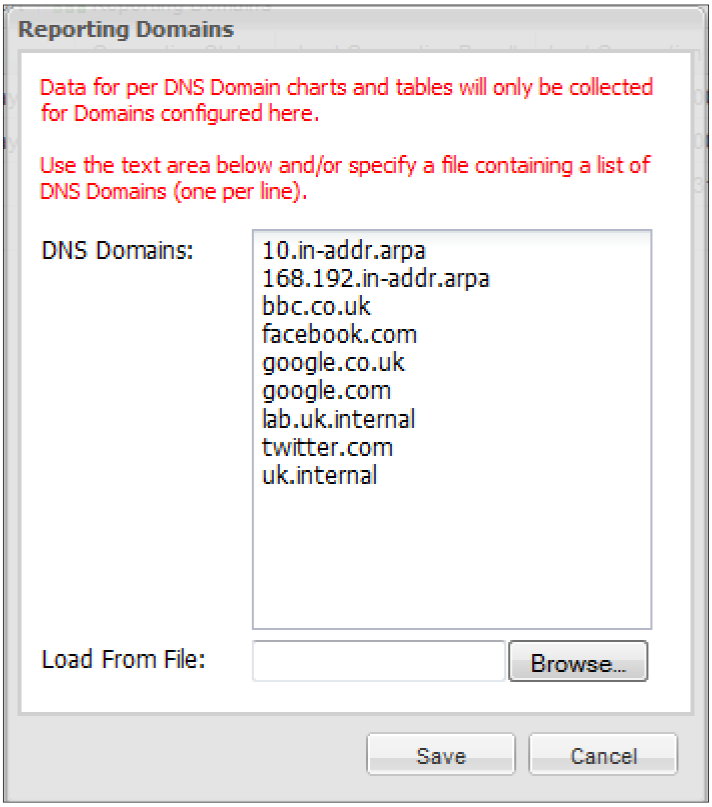
Column	Filter Type	Description
Node	N/A	Node on which the data was seen. This column is only displayed if the "Breakdown by Node" checkbox is checked under the options menu.
Domain Name	String	Domain under which the client issued a query for.
Client IP	IP Address	IP address of the DNS client in dotted quad format.
Query Count	Number	Number of queries seen from the client for the period and resolution selected.

7.2.9 Top DNS Domains

Displays the count of queries under specified DNS domains, ordered by highest first.

When processing fully qualified domain names, it is very difficult to establish which portion of the name actually represents the domain name (this is due to the wide scale use of "dotted hostnames").

Therefore in order to provide a report of "Top clients querying a domain", DDAM has to be configured with a list of domains that it can report against. These domains are called "Reporting Domains" and can be configured by selecting the "Reporting Domains" button on the "Configured Reports" tab:



Reporting Domains

Data for per DNS Domain charts and tables will only be collected for Domains configured here.

Use the text area below and/or specify a file containing a list of DNS Domains (one per line).

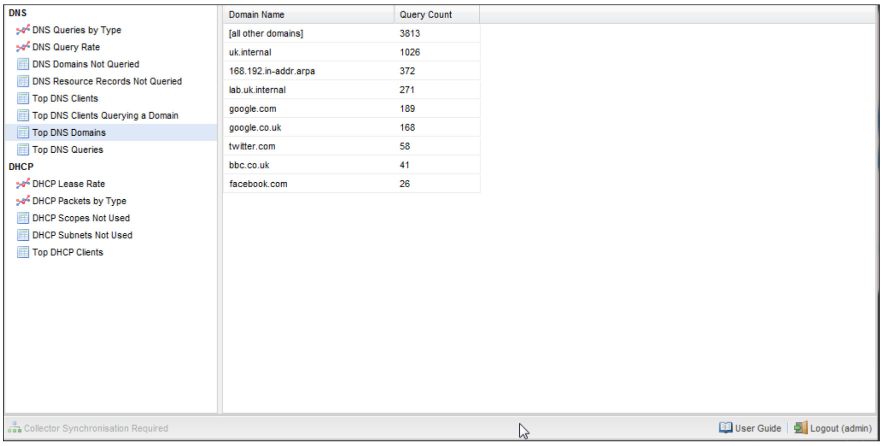
DNS Domains:

```
10.in-addr.arpa
168.192.in-addr.arpa
bbc.co.uk
facebook.com
google.co.uk
google.com
lab.uk.internal
twitter.com
uk.internal
```

Load From File:

The domain names listed in this report will depend on what reporting domains have been configured.

All queries not under any reporting domain configured will be totaled under the domain "[all other domains]".



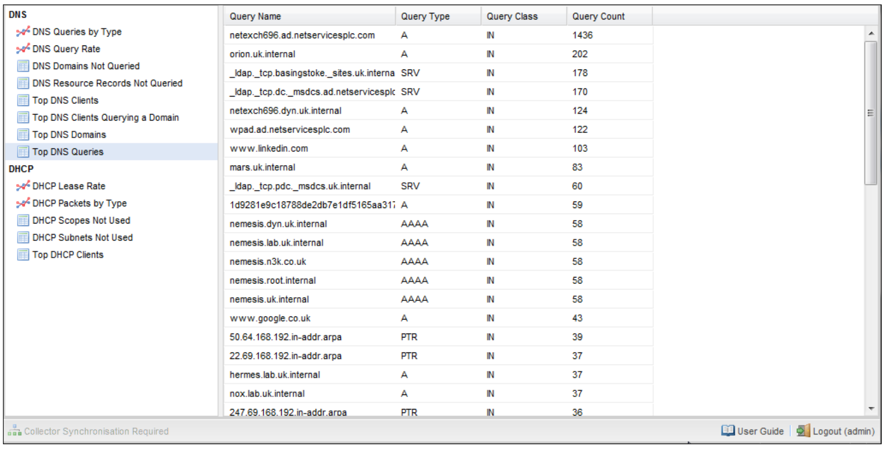
Domain Name	Query Count
[all other domains]	3813
uk.internal	1026
168.192.in-addr.arpa	372
lab.uk.internal	271
google.com	189
google.co.uk	168
twitter.com	58
bbc.co.uk	41
facebook.com	26

The following columns are available in this report:

Column	Filter Type	Description
Node	N/A	Node on which the data was seen. This column is only displayed if the "Breakdown by Node" checkbox is checked under the options menu.
Domain Name	String	Domain name.
Query Count	Number	Number of queries seen for the period and resolution selected.

7.2.10 Top DNS Queries

Displays a list of DNS queries which have been issued by one or more DNS clients, ordered by highest first.



Query Name	Query Type	Query Class	Query Count
netexch696.ad.netservicesplc.com	A	IN	1436
orion.uk.internal	A	IN	202
_ldap._tcp.basingstoke._sites.uk.interna	SRV	IN	178
_ldap._tcp.dc._msdcs.ad.netservicesplc	SRV	IN	170
netexch696.dyn.uk.internal	A	IN	124
wpad.ad.netservicesplc.com	A	IN	122
www.linkedin.com	A	IN	103
mars.uk.internal	A	IN	83
_ldap._tcp.pdc._msdcs.uk.internal	SRV	IN	60
1d9281e9c18788de2db7e1df5165aa31	A	IN	59
nemesis.dyn.uk.internal	AAAA	IN	58
nemesis.lab.uk.internal	AAAA	IN	58
nemesis.n3k.co.uk	AAAA	IN	58
nemesis.root.internal	AAAA	IN	58
nemesis.uk.internal	AAAA	IN	58
www.google.co.uk	A	IN	43
50.64.168.192.in-addr.arpa	PTR	IN	39
22.69.168.192.in-addr.arpa	PTR	IN	37
hermes.lab.uk.internal	A	IN	37
nox.lab.uk.internal	A	IN	37
247.69.168.192.in-addr.arpa	PTR	IN	36

The following columns are available in this report:

Column	Filter Type	Description
Node	N/A	Node on which the data was seen. This column is only displayed if the "Breakdown by Node" checkbox is checked under the options menu.
Query Name	String	Query name for the query.
Query Type	Enum	Query type for the query.
Query Class	Enum	Query class for the query.
Query Count	Number	Number of queries seen for the period and resolution selected.

7.2.11 DHCP Scopes Not Used

This report produces a list of DHCP scopes for which no DHCP packets have been seen for a period of time. A scope in the context of DDAM is a range of IP addresses, for example 192.168.2.1 - 192.168.2.100. The motivation for using this report is to identify redundant DHCP scopes that could potentially be removed.

DDAM looks at the ciaddr (Client IP Address) field of each DHCP packet and records the date of each IP address seen.

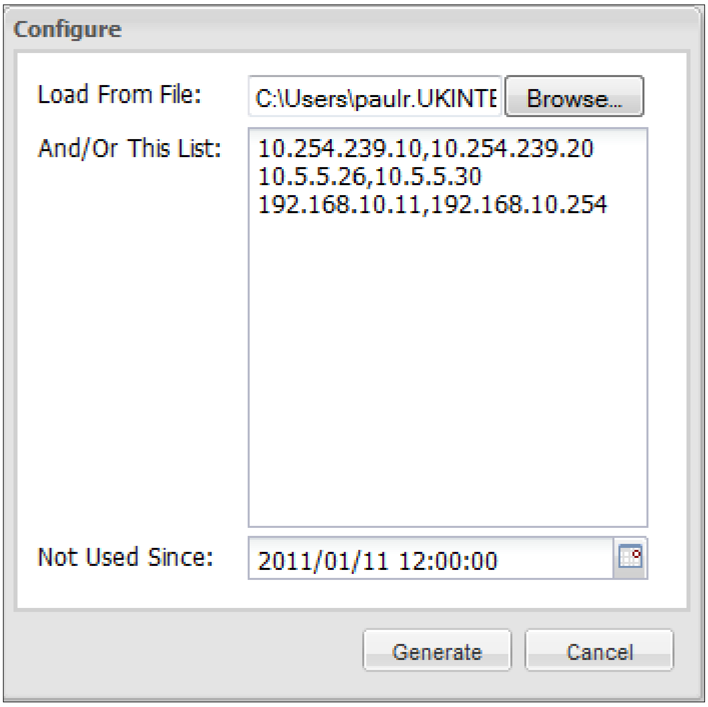
When generating data for this report, a list of scopes can be defined in a text file or a dhcpd.conf file from an Alcatel-Lucent or ISC based DHCP server can be loaded. Scopes can also be manually entered into a text box.

NOTE: If a flat text file is used, each line must contain the start and end address of each DHCP/bootp scope that is to be checked in comma separated format, for example:

```
10.254.239.10,10.254.239.20

10.5.5.26,10.5.5.30

192.168.10.11,192.168.10.254
```

The same format should also be used if scopes are entered manually into the text box.

To generate a report click the "Regenerate" button, after which a Configure dialog will be displayed. The following options can be configured under this dialog:



Load From File: C:\Users\paulr.UKINTE

And/Or This List:
10.254.239.10,10.254.239.20
10.5.5.26,10.5.5.30
192.168.10.11,192.168.10.254

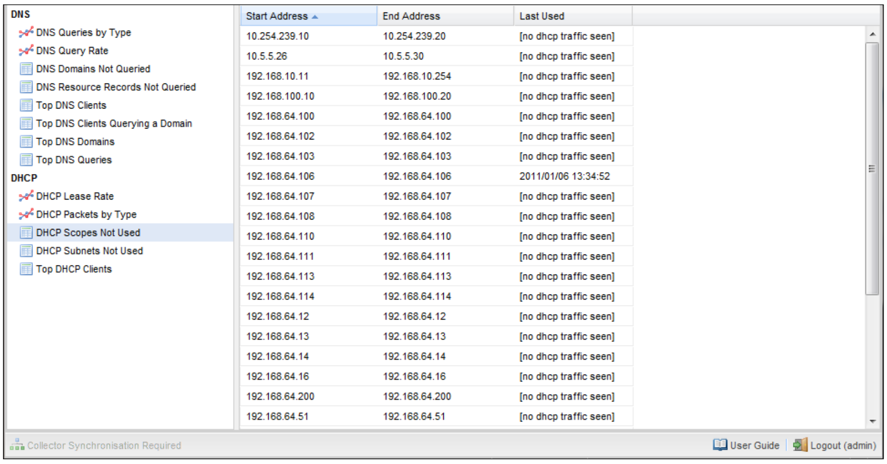
Not Used Since: 2011/01/11 12:00:00

Option	Description
Load From File	Specify a DHCP configuration file, from an Alcatel-Lucent or ISC based DHCP server, or a flat text file containing a list of DHCP address ranges.
And/Or This List	A list of DHCP address ranges (one per line).
Not Used Since	Select the date after which a scope must not have been used for a scope to be displayed in the generated report.

After the report has been configured, the "Generate" button can be clicked to generate the report.

The report will produce a list of DHCP ranges for which no packet has been seen since the date specified in the configure dialog.

Manual DHCP and bootp addresses will be displayed as a range of one IP address, e.g. the start and end address will be the same.



Start Address	End Address	Last Used
10.254.239.10	10.254.239.20	[no dhcp traffic seen]
10.5.5.26	10.5.5.30	[no dhcp traffic seen]
192.168.10.11	192.168.10.254	[no dhcp traffic seen]
192.168.100.10	192.168.100.20	[no dhcp traffic seen]
192.168.64.100	192.168.64.100	[no dhcp traffic seen]
192.168.64.102	192.168.64.102	[no dhcp traffic seen]
192.168.64.103	192.168.64.103	[no dhcp traffic seen]
192.168.64.106	192.168.64.106	2011/01/06 13:34:52
192.168.64.107	192.168.64.107	[no dhcp traffic seen]
192.168.64.108	192.168.64.108	[no dhcp traffic seen]
192.168.64.110	192.168.64.110	[no dhcp traffic seen]
192.168.64.111	192.168.64.111	[no dhcp traffic seen]
192.168.64.113	192.168.64.113	[no dhcp traffic seen]
192.168.64.114	192.168.64.114	[no dhcp traffic seen]
192.168.64.12	192.168.64.12	[no dhcp traffic seen]
192.168.64.13	192.168.64.13	[no dhcp traffic seen]
192.168.64.14	192.168.64.14	[no dhcp traffic seen]
192.168.64.16	192.168.64.16	[no dhcp traffic seen]
192.168.64.200	192.168.64.200	[no dhcp traffic seen]
192.168.64.51	192.168.64.51	[no dhcp traffic seen]

The following columns are displayed:

Column	Description
Start Address	Start address of the scope
End Address	End address of the scope
Type	Detected scope type (when loading from an Alcatel-Lucent or ISC DHCP configuration file)
Last Used	If no packet was ever seen for this scope "[no dhcp traffic seen]" will be displayed in this column, otherwise the date of the last packet seen for the scope will be displayed.

NOTE: If a particular range is not listed in the report, it is because a DHCP packet (or multiple packets) has been detected for that range since the "Not Used Since" date specified when the report was generated.

7.2.12 DHCP Subnets Not Used

This report produces a list of DHCP subnets for which no DHCP packets have been seen for a period of time.

DDAM looks at the ciaddr field of each DHCP packet and records the date of each IP address seen.

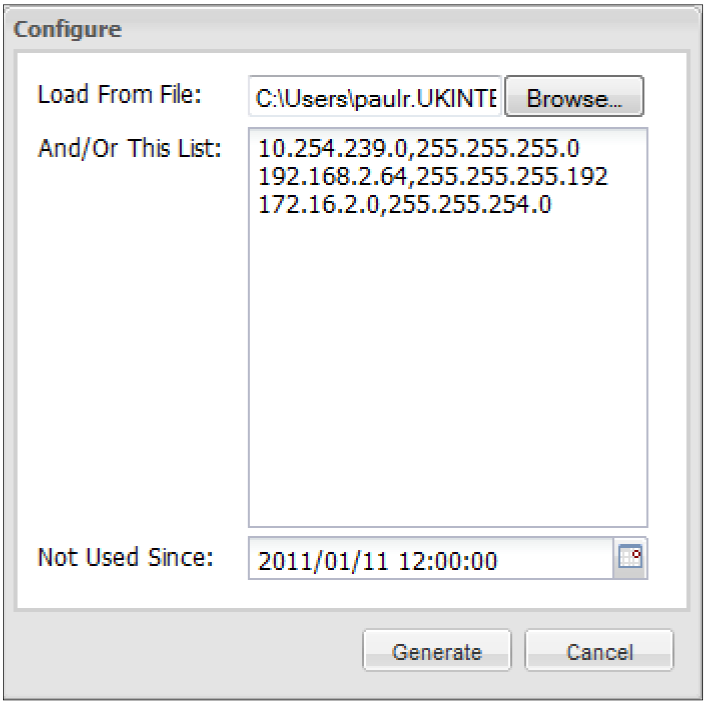
When generating data for this report, a list of subnets can be specified in a flat text file or a DHCP configuration file from an Alcatel-Lucent or ISC based DHCP server. Subnets can also be entered manually into a text box.

NOTE: If a flat text file is used, each line must contain the subnet address and subnet mask (in dotted quad format) that is to be checked in comma separated format, for example:

```
10.254.239.0,255.255.255.0

192.168.2.64,255.255.255.192

172.16.2.0,255.255.254.0
```

The same format should also be used if subnets are entered manually into the text box.

To generate a report click the "Regenerate" button, after which a Configure dialog will be displayed. The following options can be configured under this dialog:



C:\Users\paulr.UKINTE

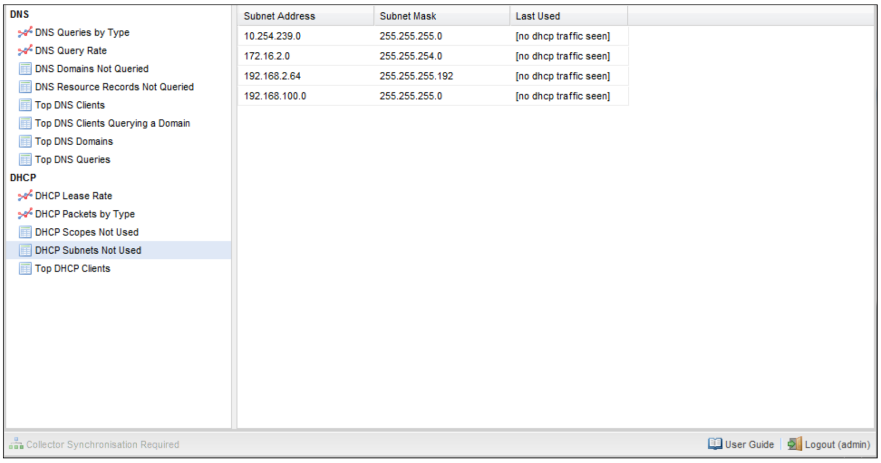
10.254.239.0,255.255.255.0
192.168.2.64,255.255.255.192
172.16.2.0,255.255.254.0

2011/01/11 12:00:00

Option	Description
Load From File	Specify a DHCP configuration file, from an Alcatel-Lucent or ISC based DHCP server, or a flat text file containing a list of subnets
And/Or This List	A list of subnets (one per line)
Not Used Since	Select the date after which a subnet must not have been used for a subnet to be displayed in the generated report.

After the report has been configured, the "Generate" button can be clicked to generate the report.

The report will produce a list of subnets for which no DHCP packets have been seen since the date specified in the configure dialog.



Subnet Address	Subnet Mask	Last Used
10.254.239.0	255.255.255.0	[no dhcp traffic seen]
172.16.2.0	255.255.254.0	[no dhcp traffic seen]
192.168.2.64	255.255.255.192	[no dhcp traffic seen]
192.168.100.0	255.255.255.0	[no dhcp traffic seen]

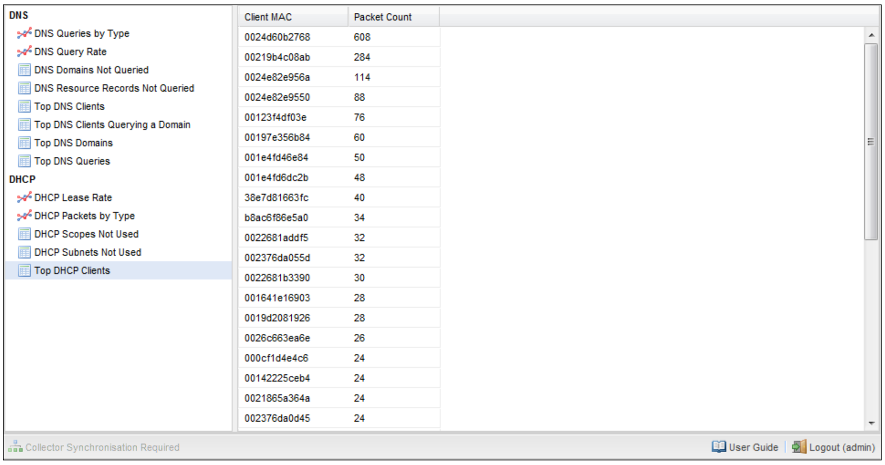
The following columns are displayed:

Column	Description
Subnet Address	Address of the subnet
Subnet Mask	Subnet mask of the subnet
Last Used	If no packet was ever seen for this subnet "[no dhcp traffic seen]" will be displayed in this column, otherwise the date of the last packet seen for the subnet will be displayed.

NOTE: If a particular subnet is not listed in the report, it is because a DHCP packet (or multiple packets) has been detected for that subnet since the "Not Used Since" date specified when the report was generated.

7.2.13 Top DHCP Clients

Displays DHCP clients, by MAC address, which have sent or received DHCP packets and the number of packets seen, ordered by highest first.



Client MAC	Packet Count
0024d60b2768	608
00219b4c08ab	284
0024e82e956a	114
0024e82e9550	88
00123f4df03e	76
00197e356b84	60
001e4fd46e84	50
001e4fd6dc2b	48
38e7d81663fc	40
b8ac6f86e5a0	34
0022681addf5	32
002376da055d	32
0022681b3390	30
001641e16903	28
0019d2081926	28
0026c663ea6e	26
000cf1d4e4c6	24
00142225ceb4	24
0021865a364a	24
002376da0d45	24

The following columns are available in this report:

Column	Filter Type	Description
Node	N/A	Node on which the data was seen. This column is only displayed if the "Breakdown by Node" checkbox is checked under the options menu.
Client MAC	String	MAC address of the DHCP client in hexadecimal format.
Packet Count	Number	Number of packets seen for the period and resolution selected.

7.3 PDF Reports

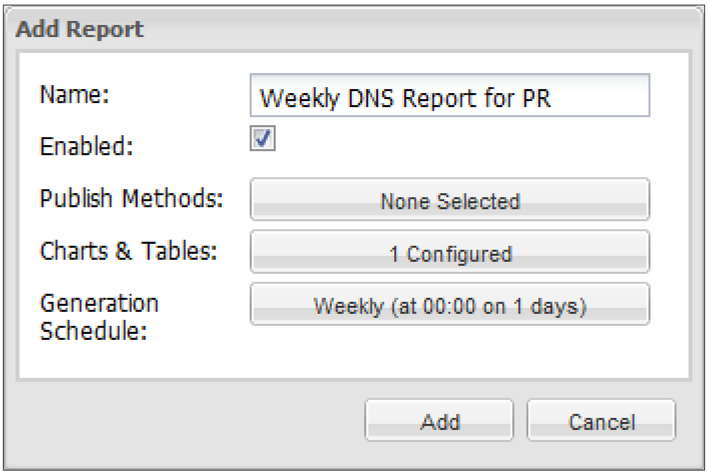
DDAM provides the ability to configure scheduled PDF report generation, and also provides the ability to customize the contents of each PDF report. A scheduled PDF report can be generated automatically at a specific time on a specific day on a recurring schedule, e.g. generate a report at 8am every Monday morning. The report can be published via email or saved to a specific location.

All charts and tables found under the Charts & Tables page, with the exception of the Last Used/Queried tables, can be included in PDF reports.

If an administrator has the appropriate privileges, PDF reports can be managed in the Reports section under the "Configured Reports" tab.

New PDF reports can be added by clicking the "Add Report" button. Existing reports can be modified by right clicking the report and selecting "Modify Report", and deleted by right clicking the report and selecting "Delete Report". If administrator privileges do not include the right to manage reports, the right click menu will not be available.

The following fields can be configured when adding and modifying a report:



Name: Weekly DNS Report for PR
Enabled: ☑
Publish Methods: None Selected
Charts & Tables: 1 Configured
Generation Schedule: Weekly (at 00:00 on 1 days)

Field	Description
Name	Name of the report. The report name will appear as the title in generated reports.
Enabled	Check this box to enable report generation as per the schedule defined for this report. If this box is left unchecked, reports will not be automatically generated but can still

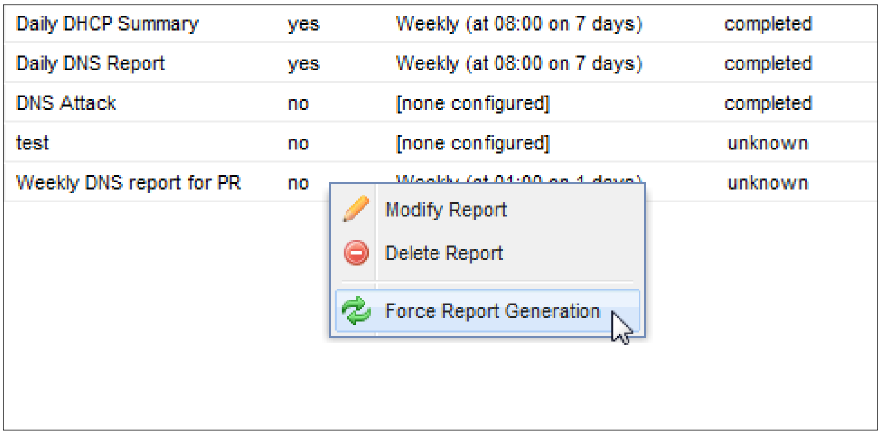
	be generated manually.
Publish Methods	This option allows a publish method to be specified for the report. This option is only available during report addition. If no publish methods are selected, the report will still be generated but it will not be published (i.e. sent via email). If the required publish method is not currently available it can be specified at a later date. After report addition, publish methods can be assigned to reports under the Reports->Configured Publish Methods tab.
Charts & Tables	Use this option to configure the contents of the report. See the "Configure Charts & Tables" section below for further details.
Generation Schedule	Use this option to configure the reports generation schedule. See the "Configure Generation Schedule" section below for further details.

Under the "Configured Reports" tab an entry for each report defined is displayed with the following columns:

Column	**Description**
Name	Name of the report, this will appear as the title in the PDF report.
Enabled	If the "Enabled" checkbox was checked during report modification or addition "yes" will be displayed, and the report will generated as per the generation scheduled. Otherwise "no" will be displayed and the system will not generate the report as per the generation schedule - users will still be able to force a report generation though.

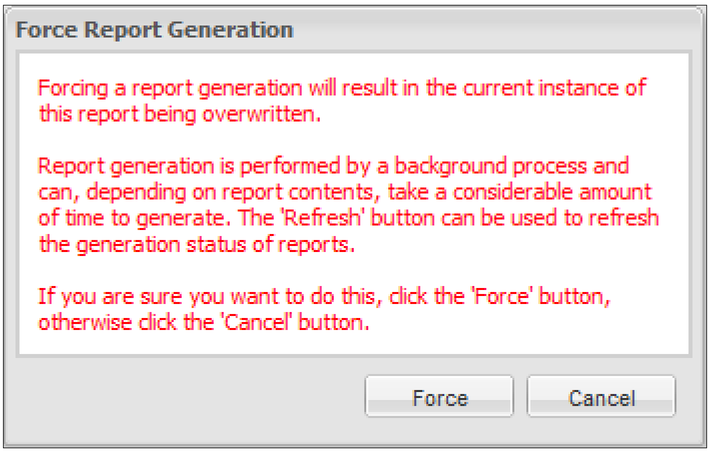
Generation Schedule	A summary of the generation schedule configured for this report. If no generation has been configured "[none configured]" will be displayed.
Generation Status	If the report has never been generated "unknown" will be displayed, if the report has been generated "completed" will be displayed, otherwise "generating" will be displayed indicating the report is currently being generated.
Last Generation Result	If the report has never been generated "unknown" will be displayed, otherwise "successful" will be displayed if the last report generation was successful, and "failed" if the last report generation failed.
Last Generation Completed At	Time at which the report was generation. If the report has not been generated "unknown" will be displayed.
Last Generation Error	If the last report generated failed, this field will indicate the reason for failure, otherwise the field will be empty.

Rather than waiting for the system to generate a report as per the report generation schedule, a report generation can be forced by right clicking a report and selecting "Force Report Generation":



Daily DHCP Summary	yes	Weekly (at 08:00 on 7 days)	completed
Daily DNS Report	yes	Weekly (at 08:00 on 7 days)	completed
DNS Attack	no	[none configured]	completed
test	no	[none configured]	unknown
Weekly DNS report for PR	no	Weekly (at 01:00 on 1 days)	unknown

When forcing a report generation, the following warning is displayed:



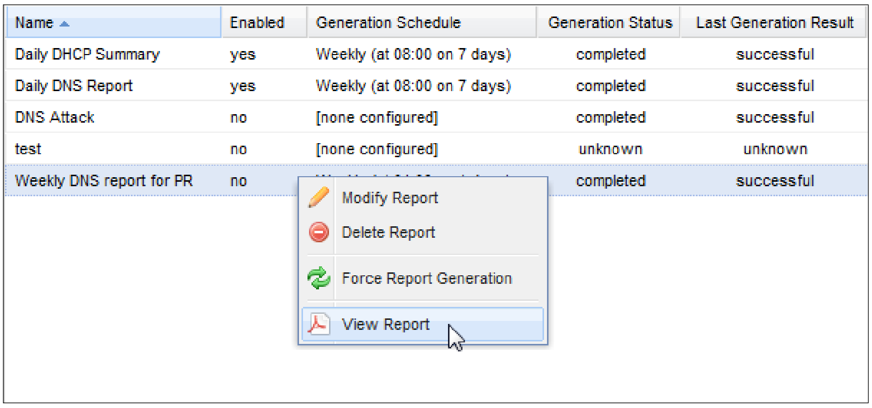
Force Report Generation

Forcing a report generation will result in the current instance of this report being overwritten.

Report generation is performed by a background process and can, depending on report contents, take a considerable amount of time to generate. The 'Refresh' button can be used to refresh the generation status of reports.

If you are sure you want to do this, click the 'Force' button, otherwise click the 'Cancel' button.

Upon clicking the "Force" button, the report generation status will move into a "generating" status (please allow time for this to occur) indicating the report is being generated. Click the "Refresh" button to update the status columns. Once a report has been generated, the option "View Report" will become available under the reports right click menu:

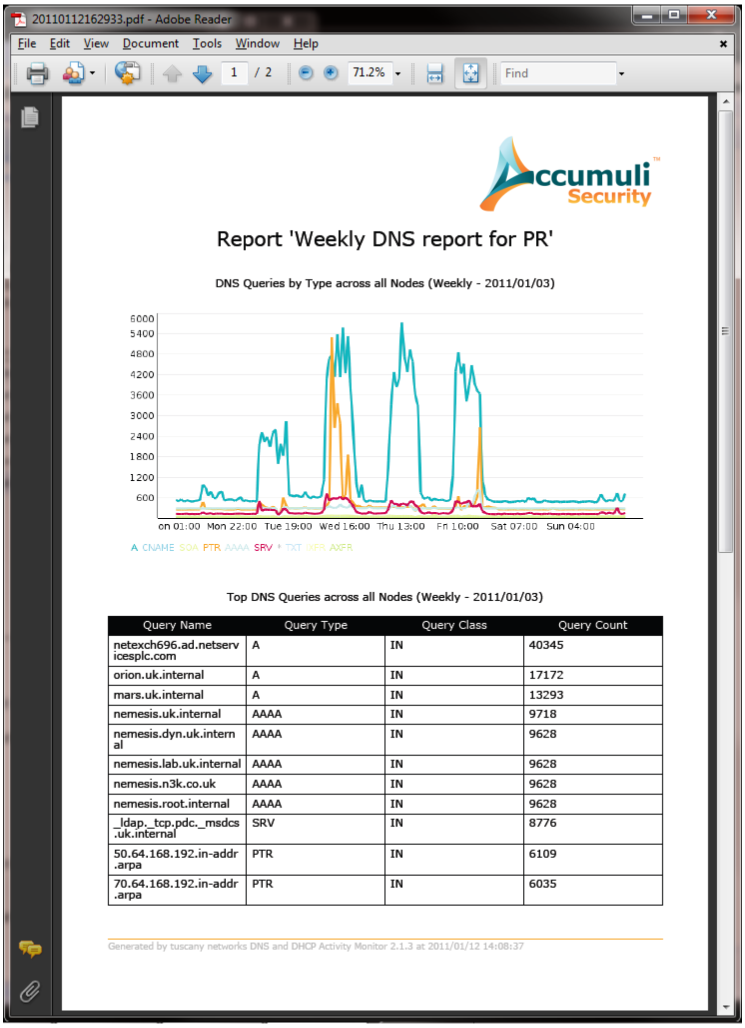


Name	Enabled	Generation Schedule	Generation Status	Last Generation Result
Daily DHCP Summary	yes	Weekly (at 08:00 on 7 days)	completed	successful
Daily DNS Report	yes	Weekly (at 08:00 on 7 days)	completed	successful
DNS Attack	no	[none configured]	completed	successful
test	no	[none configured]	unknown	unknown
Weekly DNS report for PR	no		completed	successful

***NOTE:** Adobe Acrobat Reader must be installed in order to view the report.*

Click this option to view the last PDF report generated for the report.

Only the last report is kept by DDAM. Configure one or more publish methods to keep more than one previous report instance.



Report 'Weekly DNS report for PR'

DNS Queries by Type across all Nodes (Weekly - 2011/01/03)

Top DNS Queries across all Nodes (Weekly - 2011/01/03)

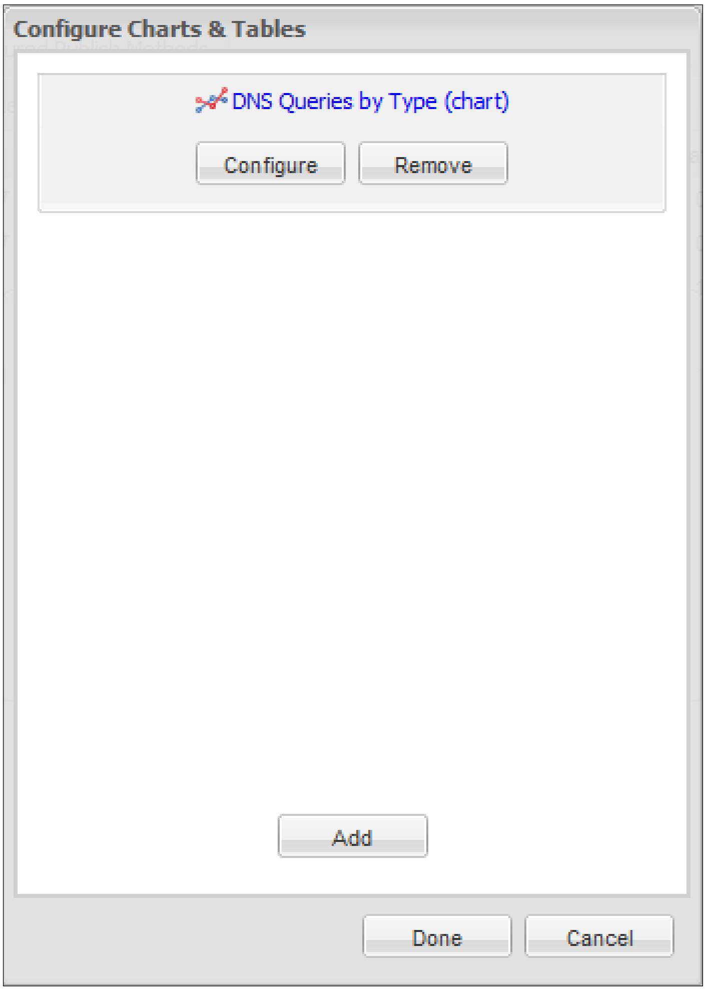
Query Name	Query Type	Query Class	Query Count
netexch696.ad.netservicesplc.com	A	IN	40345
orion.uk.internal	A	IN	17172
mars.uk.internal	A	IN	13293
nemesis.uk.internal	AAAA	IN	9718
nemesis.dyn.uk.internal	AAAA	IN	9628
nemesis.lab.uk.internal	AAAA	IN	9628
nemesis.n3k.co.uk	AAAA	IN	9628
nemesis.root.internal	AAAA	IN	9628
_ldap._tcp.pdc._msdcs.uk.internal	SRV	IN	8776
50.64.168.192.in-addr.arpa	PTR	IN	6109
70.64.168.192.in-addr.arpa	PTR	IN	6035

Generated by tuscany networks DNS and DHCP Activity Monitor 2.1.3 at 2011/01/12 14:08:37

7.3.1 Configure Charts & Tables

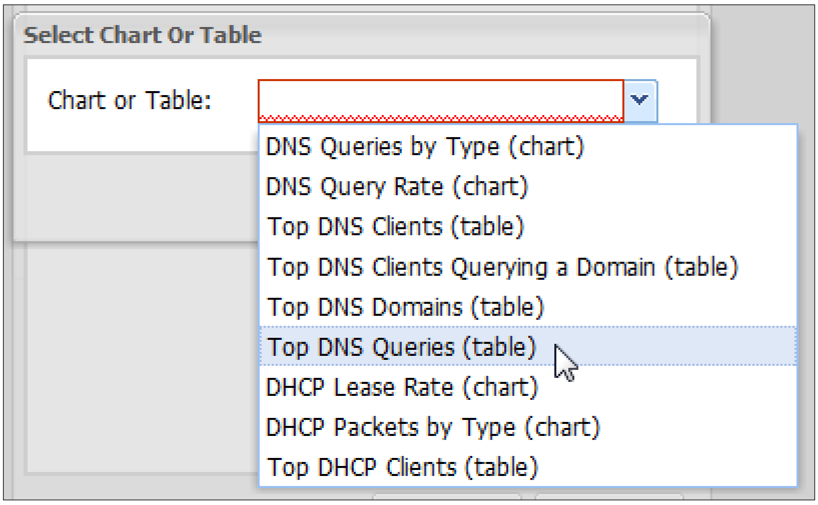
During report addition and modification the contents of reports can be configured using the "Charts & Tables" button.

Using this option causes the "Configure Charts & Tables" dialog to appear:

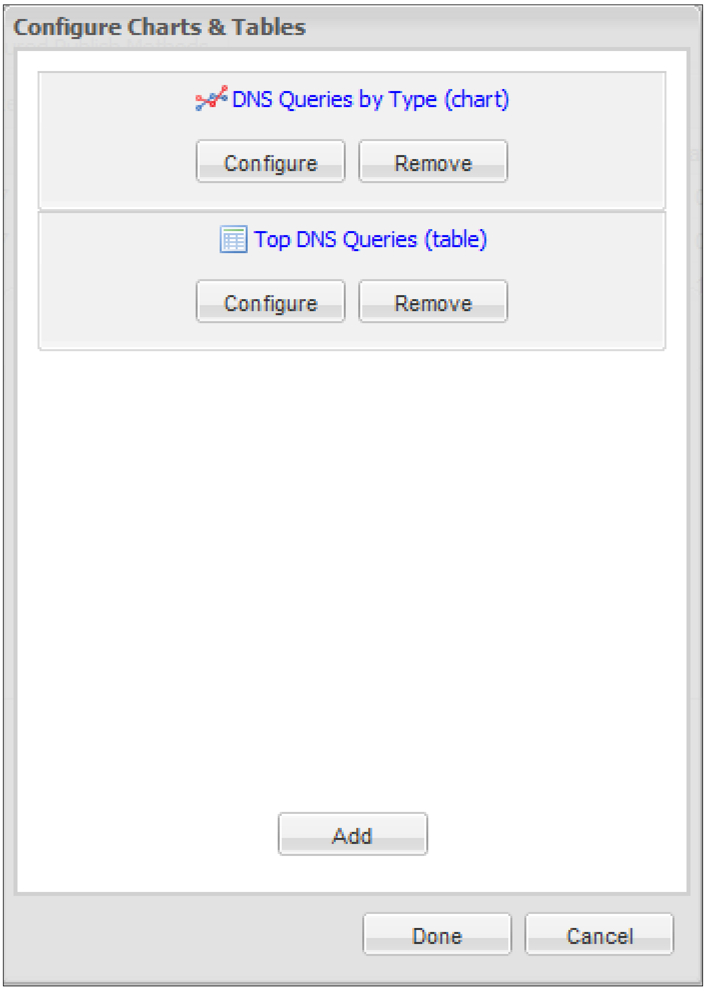


Selected charts and tables are organized on the screen in the order in which they appear in the generated report. The screen shot above shows a report that already has a chart defined but if doing this for a new PDF report, it will be blank.

Use the Add button to add a chart or table to the generated report. A drop down dialogue box will then allow a table or chart to be selected.

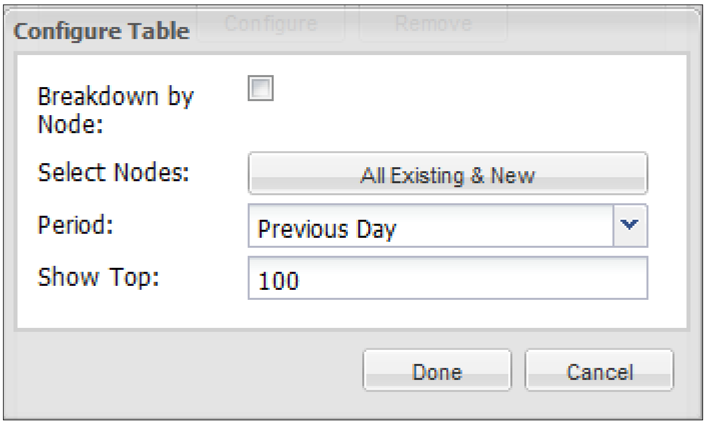


After selecting the chart or table, and clicking the Select button, the chart or table will appear on the list of selected charts and tables. The order they are listed here is the order they will be produced within the PDF report:



The Remove button can be used to remove a selected chart or table from the PDF report.

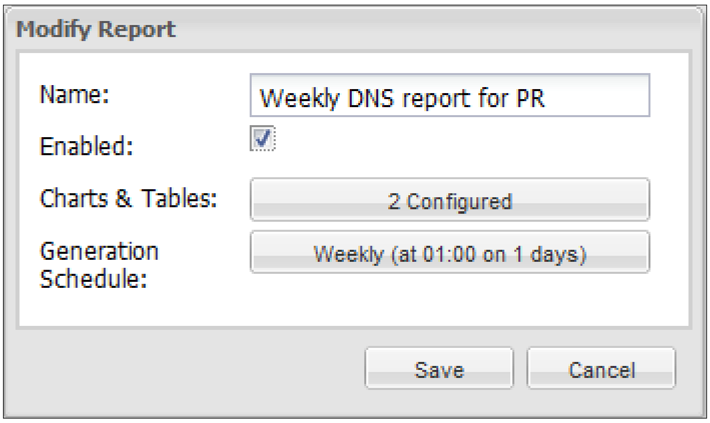
The Configure button can be used to configure additional options for each report. By default, each report will apply to all nodes, unless the "Breakdown by Node" check box is selected, or the "Select Nodes" button is used to select specific nodes. The period can be defined in order to ensure the relevant time period is used for the report. For tables, the report can be limited to the top n clients/domains/queries etc. to limit the overall length of the report:



Breakdown by Node: ☐
Select Nodes: All Existing & New
Period: Previous Day
Show Top: 100

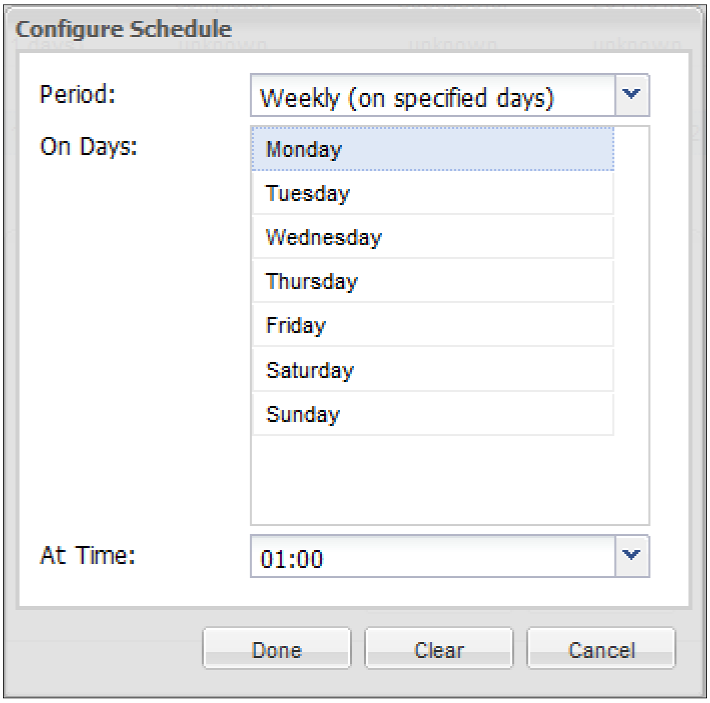
7.3.2 Configure Generation Schedule

During report addition and modification, a schedule can be defined using the "Generation Schedule" option.



Name: Weekly DNS report for PR
Enabled: ☑
Charts & Tables: 2 Configured
Generation Schedule: Weekly (at 01:00 on 1 days)

Reports can be scheduled using a weekly or monthly generation period. For instance, using a weekly period, reports can be generated at a specific time on a specific day of the week. Multiple days can be selected if required (using CTRL and left click on Windows platforms):

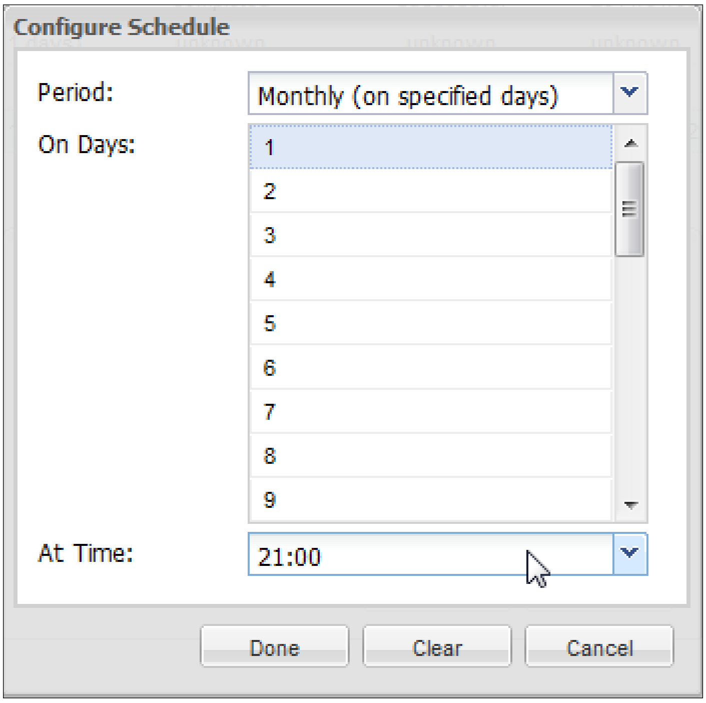


Period: Weekly (on specified days)

On Days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

At Time: 01:00

Alternatively, reports can be generated using a monthly period, meaning that specific days of the month can be selected. Multiple days can be selected if required (using CTRL and left click on Windows platforms):



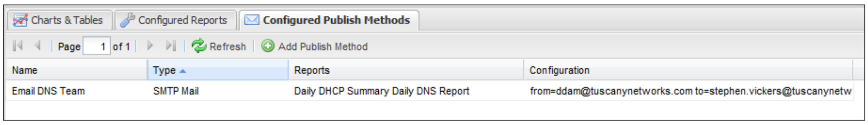
Period: Monthly (on specified days)

At Time: 21:00

The "At Time" dropdown box allows the time at which the report should be generated to be specified. The system will generate the report on, or around, the time specified. Depending on report contents some reports can take considerable time to complete.

7.4 Publish Methods

Under the "Configured Publish Methods" tab, it is possible to manage the publication methods that are used to publish generated reports from the system.

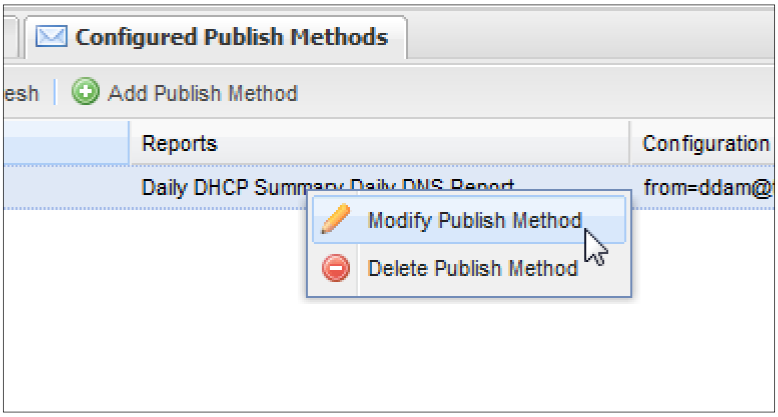


Name	Type	Reports	Configuration
Email DNS Team	SMTP Mail	Daily DHCP Summary Daily DNS Report	from=ddam@tuscanynetworks.com to=stephen.vickers@tuscanynetw

Column	Description
Name	Name of the publish method.
Type	Type of publish method. Currently only "Local

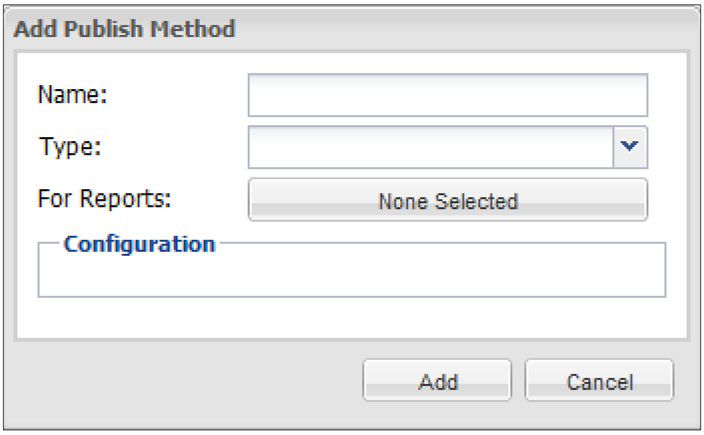
	file system" and "SMTP Mail" are supported.
Reports	A list of Reports the publish method is configured for. Multiple reports will be separated with a space.
Configuration	A list of key/value pairs detailing the configuration of the publish method. The contents of this field will be different for each type of publish method.

Publish methods can be added by clicking the "Add Publish Method" button. Existing publish methods can be modified or deleted by using a right click menu.



Daily DHCP Summary Daily DNS Report
from=ddam@

The following fields can be configured when adding or modifying a publish method:



Field	Description
Name	Name of the publish method.
Type	Type of publish method to add.
For Reports	Use this button to select which Reports will be dispatched from the system, upon generation, using this publish method. If a report was previously configured with no publish methods, the report can be selected from this list to associate it with this publish method.
Configuration	This field set will contain a number of configurable options relevant to the type of publish method that was selected in the "Type" field.

7.4.1 Available Publish Methods

The following Publish Methods can be configured:

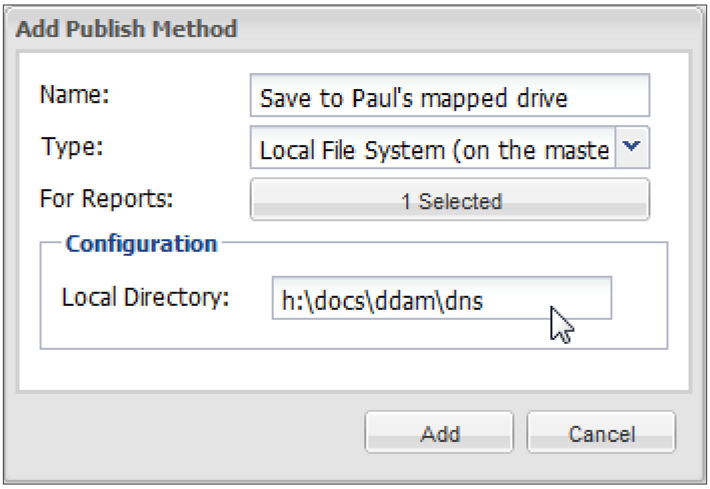
7.4.1.1 Local File System

__NOTE:__ This directory could be located under a Unix NFS mount point or Windows network mapped drive letter.

Configuring this Publish Method and associating reports with it will result in the system placing a copy of the generated PDF report into a specified directory on the master server.

The report filename will be in the format of "<report-name>.pdf", where <report-name> is the configured report name with all non-alphanumeric characters replaced with underscores.

The following configurable options are available for this Publish Method:



Name: Save to Paul's mapped drive

Type: Local File System (on the maste

For Reports: 1 Selected

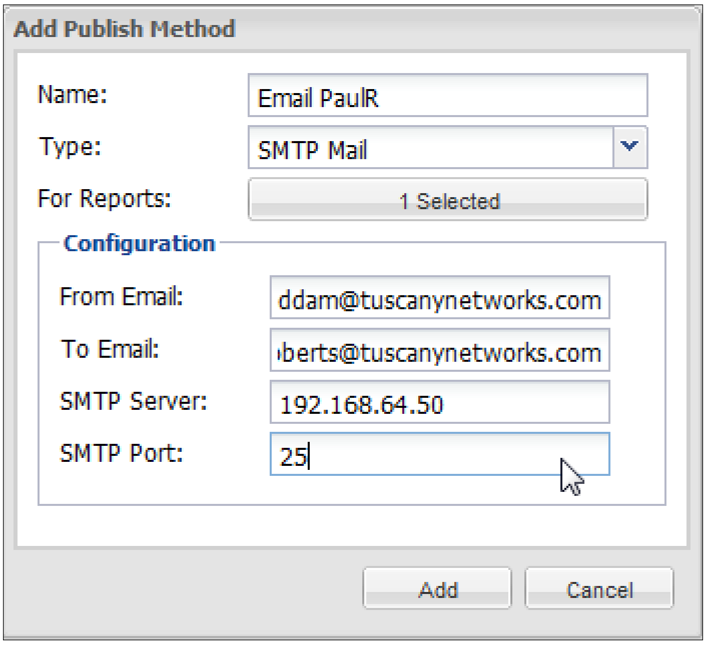
Local Directory: h:\docs\ddam\dns

Option	Description
Local Directory	Directory on the master server in which to place generated reports. The directory should already exist.

7.4.1.2 SMTP Mail

Configuring this Publish Method and associating reports with it will result in the system dispatching an SMTP mail with the generated PDF report attached.

The following configurable options are available for this Publish Method:



Name: Email PaulR

Type: SMTP Mail

For Reports: 1 Selected

Configuration

From Email: ddam@tuscanynetworks.com

To Email: ıberts@tuscanynetworks.com

SMTP Server: 192.168.64.50

SMTP Port: 25

Option	Description
From Email	Email address the emails should appear to be from.
To Email	A comma separated list of email addresses reports should be sent to.
SMTP Server	IP address or hostname of SMTP server.
SMTP Port	SMTP server port number.

Chapter

8

8 Administration

8.1 HTTPS Certificate

DDAM ships with a default certificate and private key which is found in the file "<install>/http-serverd.pem" on the DDAM master server.

This file can be replaced with a custom certificate and key so long as it is in PEM format. The PEM file must contain both a private key and certificate.

After replacing the http-serverd.pem file the http-serverd process must be restarted by using the "<install>/ctl restart" command on the DDAM master server.

8.2 Disable HTTPS Support

The user interface can be served over HTTP instead of HTTPS by commenting out the "certificate" option in the "<install>/http-serverd.conf" file on the DDAM master server and restarting the http-serverd process using the "<install>/ctl restart" command.

8.3 Change UI Port

The HTTP/HTTPS port number through which the user interface is served can be adjusted by modifying the "port" option in the "<install>/http-serverd.conf" file on the DDAM master server and restarting the http-serverd process using the "<install>/ctl restart" command.

8.4 Backup & Restore

NOTE: Copying report data between two masters in different timezones is not supported

8.4.1 Master

Stop all services and take a copy of the "<installation-directory>/master" directory and then start all services again.

To restore, stop all services, move the existing "<installation-directory>/master" directory out of the way, then put a copy of the "master" directory taken in a previous backup in its place, start all services, and then force and perform a collector synchronization to the master if it is also a collector.

8.4.2 Collector

There is no need to backup or restore any files or directories on collectors as all configuration is stored and built from the master.

To re-install a collector, simply install the collector agent on the server, then force and perform a collector synchronization to the collector.

8.5 External User Authentication

An authentication callout mechanism in DDAM allows customers to verify username and password data via a third party authentication protocol.

Three example authentication callouts are provided in the DDAM installation which can be used as is, or copied and customized as required.

Each of these callouts is located under the <install>/bin directory. The callout names and protocols offered by these callouts are as follows:

Authentication Protocol	Callout Name
Active Directory (via LDAP/LDAPS)	authad

Radius	authradius
Tacacs+	authtacacsplus

Each of the above callouts has their own configuration file which can be found under the <install> directory with the name “<callout-name>.conf”, e.g. <install>/authad.conf.

To enable a specific callout edit the <install>/global.conf file and set the “authentication_callout” option to the exact location of the callout, e.g.:

```
authentication_callout = /opt/ddam/bin/authradius
```

This callout will be invoked each time a user attempts to login to DDAM.

8.5.1 Custom Authentication Callouts

Custom authentication callouts can be implemented to enhance existing callouts or provide new authentication protocols.

NOTE: Currently only callouts written in the Perl programming language are supported. To use a programming language other than Perl would require a thin Perl wrapper program to pass on the authentication callout request.

Upon invoking an authentication callout DDAM passes the username and password, as provided by the user, to the STDIN of the authentication callout.

DDAM then reads one line of output from the STDOUT of the authentication callout. The authentication callout must emit one of the three status strings to its STDOUT:

- “AUTH” – authentication was successful
- “DEFER” – authentication should be performed by DDAM

- “NOAUTH” – authentication was unsuccessful (the user is denied access)

For the “AUTH” status, DDAM can be instructed to login the user as a different username to the one supplied by the user.

This feature can be useful in the case many users can login under the same username and need not require their own account, e.g. a common read-only account.

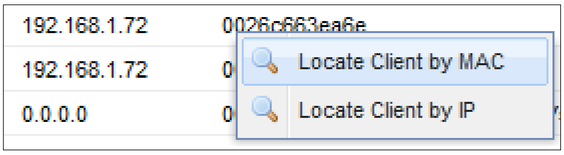
The new username is passed back to DDAM by appending the username to the status string separating it with the “:” character, for example:

```
#! perl

my $user = <>;
my $pass = <>;

s/^\s+|\s+$//g for $user, $pass;

if ($user eq “someone”) {
   print “AUTH:readonly\n”;
} else {
   print “AUTH\n”;
}
```

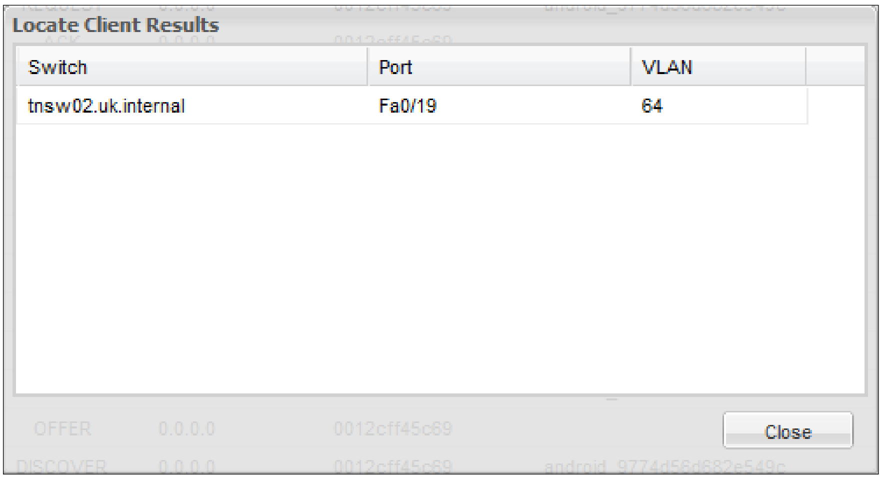
Trailing whitespace following the new username is ignored.

8.6 Enable Client Location

DDAM provides the facility to callout to an inventory product (such as porttracker or PortIQ) to support client location on the network. If the client location feature is enabled (this feature is disabled by default) a menu will be made available when right clicking an activity entry within the DHCP or DNS tabs on the Activity page:



Depending on what activity is being viewed, clients can be located either by IP address or MAC address. After locating a client, a "Locate Client Results" dialog is displayed detailing information on the switch, port and VLAN the client was found.



Switch	Port	VLAN
tnsw02.uk.internal	Fa0/19	64

Client location support is enabled by adding the option "client_locator" to the global.conf file on the DDAM master server. The "client_locator" option specifies the full path to a Perl based program which is called upon request.

An example client location script named "client-locator-pt" can be found under the "<install>/bin" directory on the DDAM master server. This script can be used to make a call out to the PortIQ or porttracker products. This can be enabled by adding the following entry to the "<install>/global.conf" file (where <install> is the installation path of DDAM on the DDAM master server):

```
client_locator = <install>/bin/client-locator-pt
```

There is no need to restart any processes.

Two parameters are passed to the client locator script. The first parameter specifies whether client location should be performed by MAC address or IP address. The parameter will specify "mac" or "ip" dependent upon the type of query being performed.

The second argument passed to the client locator script will be the MAC address or IP address of the client that should be located.

If client location fails, the client location script should exit with a non-zero exit code. If client location is successful the client location script should print to its standard output a number of rows.

Each row represents a single location where the client was found. The following is example output:

```
1|switch1|Fa0/1|64
2|switch2|Fa0/1|69
```

Each row is split up into the four fields separated by the "|" character. The first field is an ID; this should be unique for each row. The second field is the name of the switch the client was found on. The third field is the name of the port the client was found on. Finally, the fourth field is the VLAN number the client was found on.

Chapter

9

9 Troubleshooting & Support Information

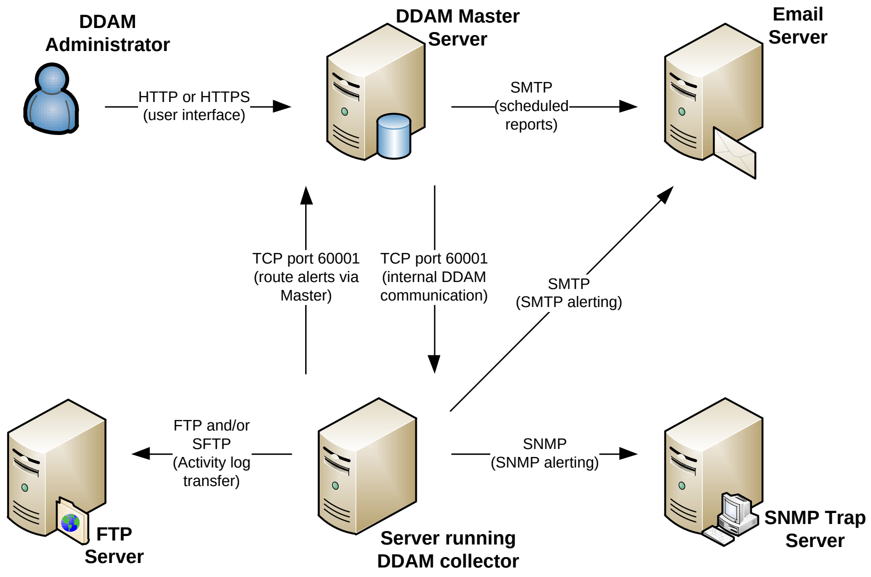
9.1 support-info.txt

This file, which can be found under the installation directory, contains information for support and troubleshooting.

The file contains information such as Node and Collector ID to name mappings to make it easier to associate activity, alerts and report data to collectors and nodes.

9.2 TCP Ports

The following diagram depicts the various TCP/UDP ports that DDAM uses:


DDAM Administrator
HTTP or HTTPS (user interface)
DDAM Master Server
SMTP (scheduled reports)
Email Server
TCP port 60001 (route alerts via Master)
TCP port 60001 (internal DDAM communication)
SMTP (SMTP alerting)
FTP and/or SFTP (Activity log transfer)
SNMP (SNMP alerting)
FTP Server
Server running DDAM collector
SNMP Trap Server

9.3 Services & Daemons

This section defines the various daemons and services that are installed.

9.3.1 DDAM Master Server

DNS and DHCP Activity Monitor HTTP Server Service (http-serverd)

Responsible for serving the user interface.

DNS and DHCP Activity Monitor Message Service (msgd)

Responsible for communication between various product components.

DNS and DHCP Activity Monitor Download Service (download)

Responsible for downloading alert and report data from collectors, generating and publishing PDF reports.

9.3.2 DDAM Collector

DNS and DHCP Activity Monitor Alert Service (alertd)

Responsible for dispatching generated alerts from collectors.

DNS and DHCP Activity Monitor Message Service (msgd)

Responsible for communication between various product components.

DNS and DHCP Activity Monitor Transfer Service (transferd)

Responsible for transferring activity logs to external systems. This service also ensures only 1 hour of activity is kept on collectors by pruning activity logs.

DNS and DHCP Activity Monitor Collector Service (colld)

Responsible for collecting DNS and/or DHCP activity and generating alerts.

9.4 Directory Structure

The following table outlines the top-level directory structure of a DDAM installation:

Directory	Description
bin	All daemons/services and command line programs.
collector	Data files created by collector processes, this includes generated alerts, activity and report data.
lib	Perl libraries files used throughout the product.
log	All daemon/service log files.
master	All product configuration, alert data and report data.

perl	Perl distribution used by the product.
tmp	Where temporary files are created.
www	User interface files.

The same directory structure is used for both masters and collectors. The presence of the "is_master" and "is_collector" files under the installation directory dictates how the installation will behave.

9.5 Enable Verbose Logging

To enable verbose logging on a specific process, edit the <install>/global.conf file and adjust the "verbose" option - typically this can be set to "100". Then restart the relevant process by running the following command while under the installation directory:

```
cd <install>
./ctl restart <daemon>
```

For the http-serverd and colld processes edit the http-serverd.conf and colld.conf files, respectively, and set the "verbose" option to "1". Then restart the relevant process by running the above command.

For Windows platforms, simply restart the service using the Windows Service Control Manager in place of running the "./ctl restart <daemon>" command.

Revert the above changes to disable verbose logging.

9.6 Unlocking a User Account

If all users have been accidently locked the “unlock-user” utility can be used to unlock a user.

This utility is located under the <install>/bin and run as follows:

```
cd <install>
./cli bin/unlock-user <username>
```

Appendix

A

Appendix A – DHCP Message Types

```
1  DISCOVER
2  OFFER
3  REQUEST
4  DECLINE
5  ACK
6  NAK
7  RELEASE
8  INFORM
10 LEASEQUERY
11 LEASEUNASSIGNED
12 LEASEUNKNOWN
13 LEASEACTIVE
```

Appendix

B

Appendix B - DNS Query Types

The following list was obtained from http://www.iana.org/assignments/dns-parameters.

```
0 RRTYPE
1 A
2 NS
3 MD
4 MF
5 CNAME
6 SOA
7 MB
8 MG
9 MR
10 NULL
11 WKS
12 PTR
13 HINFO
14 MINFO
15 MX
16 TXT
17 RP
18 AFSDB
19 X25
20 ISDN
21 RT
22 NSAP
23 NSAP-PTR
24 SIG
25 KEY
26 PX
27 GPOS
28 AAAA
29 LOC
```

```
30 NXT
31 EID
32 NIMLOC
33 SRV
34 ATMA
35 NAPTR
36 KX
37 CERT
38 A6
39 DNAME
40 SINK
41 OPT
42 APL
43 DS
44 SSHFP
45 IPSECKEY
46 RRSIG
47 NSEC
48 DNSKEY
49 DHCID
50 NSEC3
51 NSEC3PARAM
55 HIP
56 NINFO
57 RKEY
99 SPF
100 UINFO
101 UID
102 GID
103 UNSPEC
249 TKEY
250 TSIG
251 IXFR
252 AXFR
253 MAILB
254 MAILA
255 *
32768 TA
32769 DLV
```

Appendix

C

Appendix C - DNS Query Classes

The following list was obtained from http://www.iana.org/assignments/dns-parameters.

```
1   IN   (Internet)
3   CH   (Chaos)
4   HS   (Hesiod)
254 NONE
255 *    (ANY)
```

Appendix
D

Appendix D - Software Licenses & Credits

OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Please refer to the <install>/www/doc/license-openssl.txt file for the OpenSSL license.

Silk Icons

Many of the user interface icons are taken from the Silk icon set from the famfamfam website: (http://www.famfamfam.com/lab/icons/silk/).