Emerald

Network Collector
Version 4.0

Emerald Management Suite

IEA Software, Inc.

Table Of Contents

Purpose

This document describes the proposed Design and Specification for the Emerald Network Collector (EmerNet).

Overview

EmerNet is an extensible filter and aggregation module to the Emerald Management Suite that allows Emerald to summarize and bill for network traffic and other data sources.

Modules

EmerNet is designed to be modular and allow for multiple front-end sources. Each source is supported via a plugin module that translates the source into a commo n object to which EmerNet can understand and process. Currently EmerNet has modules to read in IPTraf normal and compacted log formats (IEA modifications to the original IPTraf log format). EmerNet can also listen for live NetFlow UDP packets on the defined port.

Installation

You can install EmerNet as part of the Emerald distribution by selecting the EmerNet component. You must select custom or complete from the components window, as the EmerNet component is not installed with the typical selection.

Alternately, if you have Emerald already installed, you can copy the emernet.exe file to your Emerald directory. Once copied there, start EmerNet in configuration mode (see the configuration section) and select the install button (win32 only).

Configuration

Configuring EmerNet is accomplished via the EmerNet Configuration server. To start the EmerNet Configuration server in initial configuration mode follow these steps:

1. From your Start Menu, Program Files, Emerald, Server menu, select EmerNet Server.
2. From your Start Menu, Program Files, Emerald menu, select EmerNet Config.

Alternately (if you are manually installing EmerNet):

1. Open a command prompt and change to the directory where you installed EmerNet. Within that directory, execute the command “emernet –config”.
2. Open a web browser and go to the URL: http://127.0.0.1:8018

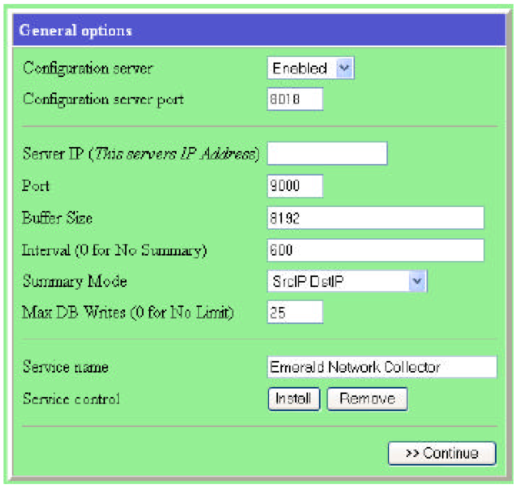
3. Select the General options menu option. After changing the settings, click continue.

   ?? Enable the Configuration Server and select a port. The default port is 8018.

   ?? If your server has more than one IP address and you want to bind to a specific IP address, enter that IP address in the Server IP. Also specify the port you will be listening for NetFlow packets on.

   ?? Set the buffer size to the size of the UDP buffer space to allocate.

   ?? If you do not want EmerNet to summarize packets for you, then set the interval value to 0. Otherwise, set the Interval value to the largest amount of time a set of packet can be summarized to a single packet. Summaries are always hourly grouped, but by



General options

Configuration server: Enabled
Configuration server port: 8018
Server IP (*This servers IP Address*):
Port: 9000
Buffer Size: 8192
Interval (0 for No Summary): 600
Summary Mode: SrcIP DstIP
Max DB Writes (0 for No Limit): 25
Service name: Emerald Network Collector
Service control

setting an interval less than one hour, you will force EmerNet to send the summary records to the DB each interval. If your interval is > 0, you can select a summary mode as well:

SrcIP/Port DstIP/Port: This will cause the largest number of records in the database, but retains the IP address and port of both the Source and Destination. Values for protocol will be 0 for all summarized records.

ScrIP DstIP This is the default mode and will summarize all records from an IP to another IP into one record, regardless of ports. A normal TCP session will have two summary records, one for each direction. Values for source port, destination port, and protocol will be 0 for all summarized records.

FilterID This is the least number of records in the database. All values for the record will be 0, except for the bytes and packets. This is full summary mode, and is the fastest and most compact of all summary modes. However, you loose all traffic details in this mode.

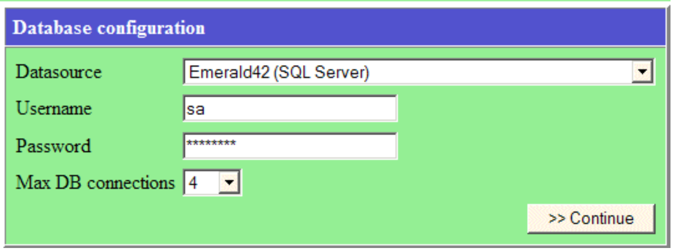
?? If you would like to restrict the number of records EmerNet can insert into the database at one time, set a value other than 0 for Max DB Writes. Setting a value of 0 will allow EmerNet to insert any number of records into the database at one time. If your summary interval is set for a large number of seconds and your summary mode is not FilterID, EmerNet can store a large number of records in the aggregation cache. Setting this value will prevent EmerNet from overloading your SQL Server when a large number of records expire from the cache around the same time.

?? Set the service name if you are going to install or remove the service. You can select the Install and Remove options to install and remove the service.

4. Select the Database Configuration menu option. After changing the settings, click continue. Please note, these settings are commonly shared between all Emerald servers. Therefore, if you already have Emerald or other Emerald server installed and configured on this machine, these settings should already be set. Changing these settings will affect all other applications as well.

?? Select a data source item. This is the ODBC DSN that you will use to connect to the Emerald database. If you do not have a DSN defined, you can select (new) to create a new DSN.

?? Fill in the username and password to connect to the database as.


Database configuration

Datasource: Emerald42 (SQL Server)
Username: sa
Password: ********
Max DB connections: 4

?? Select the number of maximum number of simultaneous database connections. The Network collector may not use all of the connections, as this is just a maximum limit it can use if needed.

5. Select the Licensing menu option and enter your license information. After changing the settings, click continue.

6. If you want to define debugging or logging, select the Debug and log menu option. You can define a server to send syslog notices to, as well as choose definite log levels. After changing the settings, click continue.

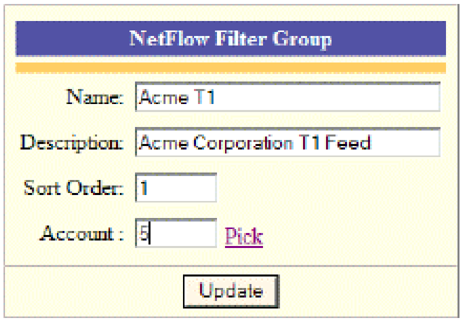
7. Once you have configured the server, it is very important that you choose the “Save Changes” Save Changes option from the top. Until you select this link, the options and changes you made will not be permanently stored. Also selecting the save changes links signals the server to reload the configuration options and start running under the new options.

Filter Definitions

In order for EmerNet to accept a record, it must match a defined filter in the database. However, before you can define a filter, you must define a filter group. Filter groups are a set of filters that are associated to a specific service in Emerald. This allows Emerald to associate the usage data and bill the respective service.

Filter Groups

You define a filter group from the Emerald Administrator, System section. Select the Flow Filter Group link to open the list of Flow Filter Groups currently defined. To add a new Group, select the new link. To edit an existing group, select the group from the list.


NetFlow Filter Group

Name: Acme T1

Description: Acme Corporation T1 Feed

Sort Order: 1

Account : 5

Name	Name of Filter Group
Description	Description of Filter Group
Sort Order	Sort Order. (See Filter Sort Order below for more information on this)
Account	The Service ID to associate this Filter Group to. You can click on the pick option to search for the service and have it automatically filled in for you.

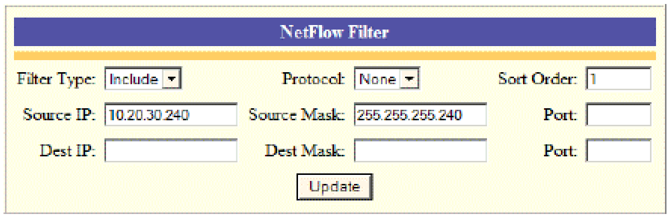
Once all information is entered, select Update to create or Update the Filter Group.

Although you do not have to pick an Account, if you want to billing for usage the Filter Group must be associated to a service. If you initially do not assign a service, and then later edit the filter group and assign a service, only those records collected after you assigned the service will be used when processing usage based billing.

Filters

Filters are used to determine whether a packet should be logged or discarded. A large number of filters can have a performance impact. As you will see later, the order of the filters are very important, as the first filter that is found to match will be used, and no other filters will be searched for. A packet can only be associated to one filter (the first one found that matches).

To create or edit a filter, first select the Filter Group to which the filter will belong to from the filter group list. Click on the Filter Group and you will see a list of filters belonging to that Filter Group. To add a new filter, select the new link. To edit an existing filter, select the filter from the list.


NetFlow Filter

Filter Type: Include

Protocol: None

Sort Order: 1

Source IP: 10.20.30.240

Source Mask: 255.255.255.240

Port:

Dest IP:

Dest Mask:

Port:

Filter Type	If set to exclude, matching records will be ignored (no further filters will be searched for). Otherwise, matching records will be kept.
Protocol	Protocol to match on. Set to none to match any protocol.
Sort Order	Search Order for filter. Filters are search in order of their Filter Group Sort Order, then the Filter Sort Order. The first matching filter is used (no further filters will be searched for). All filters in the Filter Group are searched, before checking the Filter Group with the next highest sort order. The sort order is searched from lowest to highest value.
Source IP	Source IP Address to match on. Leave blank for all IP addresses.
Source Mask	Mask to apply to Source IP Address. Set to 255.255.255.255 for a single IP address match.
Source Port	Source Port to match on. Leave blank for all ports.
Dest IP	Destination IP Address to match on. Leave blank for all IP addresses.
Dest Mask	Mask to apply to Destination IP Address. Set to 255.255.255.255 for a single IP address match.
Dest Port	Destination Port to match on. Leave blank for all ports.

Once all information is entered, select Update to create or update the Filter.

Filter Ordering and Performance

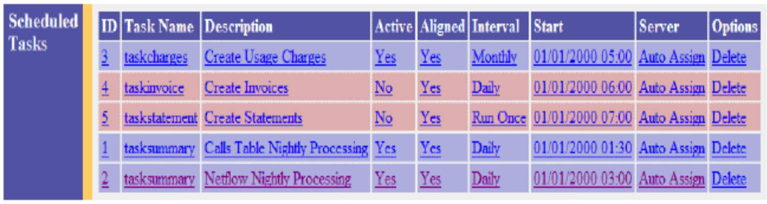
Creating a larger number of filters can have a negative performance. There are several ways to improve performance with a large number of filters:

?? Create a Filter Group with the lowest Sort Order. Inside this filter group, add only exclude filters matching subnets or traffic that you do not want to collect data for. This is only useful if you are collecting for a large number of specific filters, and you have more traffic that is not matching filters than do match filters.

?? Order your filters in order of traffic. You can do a summary of the Flows table based on FilterID and what FilterGroups they belong to. Then move those filter groups to have a lower sort order than filter groups with less traffic.

Billing

Billing for Network collected data is handled the same as any other data. The only exception is that you must make sure your NetFlow nightly processing scheduled task is enabled in the Configured Schedules section of the Admin. If that schedule is not enabled or configured, the summary of the records will not be available, preventing the billing engine access to the records.



Scheduled Tasks

ID	Task Name	Description	Active	Aligned	Interval	Start	Server	Options
3	taskcharges	Create Usage Charges	Yes	Yes	Monthly	01/01/2000 05:00	Auto Assign	Delete
4	taskinvoice	Create Invoices	No	Yes	Daily	01/01/2000 06:00	Auto Assign	Delete
5	taskstatement	Create Statements	No	Yes	Run Once	01/01/2000 07:00	Auto Assign	Delete
1	tasksummary	Calls Table Nightly Processing	Yes	Yes	Daily	01/01/2000 01:30	Auto Assign	Delete
2	tasksummary	Netflow Nightly Processing	Yes	Yes	Daily	01/01/2000 03:00	Auto Assign	Delete

When you are defining a Rate for a service that has a filter group assigned to it, the rate must be a data rate. There is no time usage collected via EmerNet, so a time rate will not work. Also, if you want to have a user that has both RADIUS usage and EmerNet usage billed, you must create two separate services, as a service can only have on rate defined to it.

To learn more about configuring rates, service types, and charges, please see the Emerald Administrator Documentation.

Configuring NetFlow Clients

There are many choices for NetFlow clients. Most Cisco routers are capable of sending NetFlow packets based on a global and interface configuration. Alternately there are several network monitoring packages that can also send NetFlow packets if you do not want to enable NetFlow on your router or you do not have a router capable of NetFlow.

There are several versions of flows that you have routers send. The three main versions are V1, V5, and V7. Although each version contains slightly different data, all three contain the base information that EmerNet needs to perform filter and aggregation functions. Additionally, there is also a V8 flow version. The main different between V8 and the other formats is that V8 allows the router to aggregate traffic and send only summary packets to the collector. This can greatly decrease network traffic between your NetFlow client and EmerNet, but at the cost of loosing detail of the traffic. If you wish to filter based on port or protocol, you cannot use the V8 version, as it does not have port or protocol information.

For more information on NetFlow formats and their abilities, please see the following URL on the Cisco website:

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

Cisco Routers

To configure a Cisco router for NetFlow requires two steps:

1. Enable NetFlow at the Global level. You will define the version of the flow to send and what address to send the flow to.

2. Enable NetFlow per interface you want to collect statistics for.

For more information on configuring NetFlow switching in a Cisco router, please see the follow URL on the Cisco website:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt3/xcdnfc.htm

ntop

ntop is a network monitoring utility that can send NetFlow packets. You can find out additional information about ntop from the ntop website:

http://www.ntop.org

You will need to obtain and compile/install ntop on a supported system. It does not have to be on the same system you installed Emerald on, as ntop will talk to EmerNet over the network.

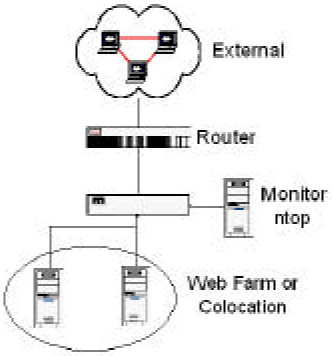
To start ntop with NetFlow enabled, add "-g host:port" to the command line used to start ntop. For example:

```
ntop -d -w 3000 -W 3001 -P /usr/local/share/ntop -g 1.2.3.4:9000
```

would start ntop in daemon mode, listen on web port 3000 and 3001 for web requests (http and https, respectively), using /usr/local/share/ntop as its work directory and sending NetFlow to host 1.2.3.4 on port 9000.

For more information on ntop, please see the ntop website listed above.

Network Monitoring



You need to plan where to enable or place a NetFlow client on your network. In a simple scenario, you can enable NetFlow at your Internet or external connection. This will send all traffic passing out through the Internet to your NetFlow collector. However, if you want to collect only for a limited number of computers (a web farm or co-location facility) this may cause a significant amount of unwanted traffic between the NetFlow client and EmerNet.

Another scenario possible uses a switch and a monitor system (like ntop). In this configuration, you would enable the port the monitor system plugs into to see all traffic across the switch. For Cisco switches this is often called the monitor port. For 3Com switches, this is often called the analysis port. Please consult your switch documentation for further details on how to configure this setup. If you switch does not have a monitor or analysis function, you can use a hub to accomplish the same function. You would plug into the hub a connection to the switch for your web farm or colocation, the monitor computer, and a connection to the Internet or external network. This limits the traffic the monitor sees only to that passing through the hub.

If you are using a monitor package like ntop, you do not need to install EmerNet on the same machine. However, if you are doing a large number of aggregations (interval time set high and using FilterID or Src IP/Dest IP as the summary mode) having EmerNet on the same machine can improve performance. However, if you are not doing any aggregations and writing all records to the database, having EmerNet on the same machine as your database server can reduce insert times.