Internet2 Network Analytics
Triannual Report
12-1-13 through 4-1-14

Introduction

This is the first in a series of periodic reviews of the Internet2 Network Analytics (MNA) service. The goal is to examine what is working and what isn't with an eye toward improvements and a focus on information important to the community for their decision-making process.

The network Analytics service is based around the Deepfield Service Analytics product. Network flow, in the form of Netflow v5 (and therefore sampling IPv4 flows only) from the R&E (1 in 100 sample) and TR-CPS (1 in 5,000 sample) routers are sent to the Deepfield application on a server in Internet2's Ann Arbor offices. There the data is combined with BGP and SNMP data rolled-up into a multi-dimensional cube that allows for various views and further analysis. The front-end is a modern web-based user interface.

The primary focus of the service is to provide network analytics to the Internet2 membership. A common request from the membership is for data that allows them to examine and report on how they are using their Internet2 services. From operational statistics to routine grant requirements, the data has not traditionally been easily available. A secondary focus of the service is to provide network analytics to help the internal staff manage the Internet services better, however the main focus will remain on the memberships ability to gather and analyze the data they need to manage their use of Internet2.

Report Overview:

Privacy & Security
Usage Reporting
Operational Status
Next Quarters Goals
Timeline

Privacy & Security

Netflow-based services generally generate inquiries around the security and privacy of the data, and rightly so. We have spent considerable time in the last four months in planning to address the various potential security and privacy issues while attempting to retain the ease of use of the system.

First, the Netflow records are not kept for any significant period of time. After arriving at the server the individual host records are rolled up in a more general record based around the advertised netblock, with the individual records being deleted shortly thereafter. This retains the data usefulness as a general planning tool while reasonably safeguarding the privacy of the /32 records.

Secondly, the server is located in the Internet2 Ann Arbor offices. While Deepfield encourages the use of cloud services, Internet2 has instead chosen to place a server, and data, in an office controlled by Internet2 staff . Thus, any external access (including any potential court order) will be known by management.

Third, the data available is scoped by institution. Because the data is organized in a multi-dimensional cube we can lock down one axis of the data at a very low level. We have locked down the service by AS number. This means that a user associated with a particular AS will only be able to see data who's source or destination is that AS.

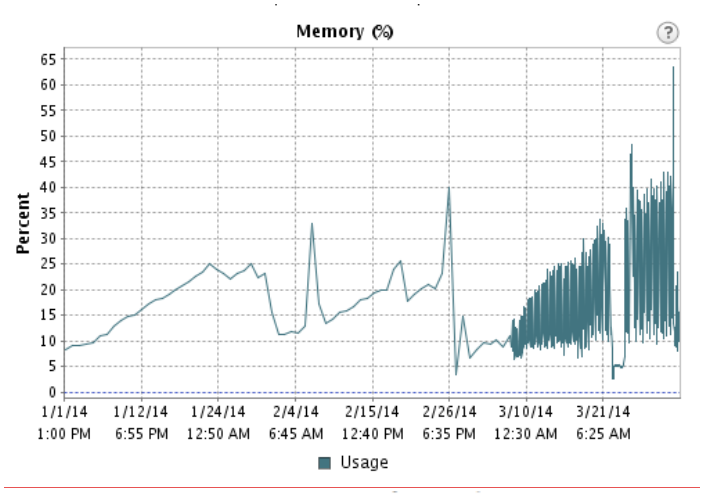
Fourth, all users of the system require executive approval to view their institutions data. Prior to adding a Shibboleth user an Approval message is sent to the members executive contact, requesting they authorize the user to view the institutions data. The response, along with the click-through agreement, is then archived.

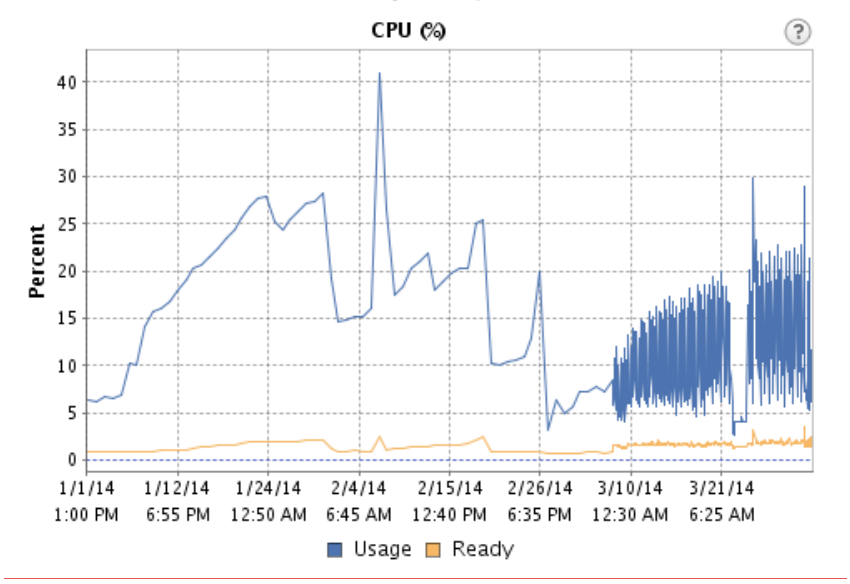
Finally, there is an internal policy which directs the staff on how they can and cannot use the data in presentations, etc.

Usage Reporting

We plan to launch the service at the 2014 Global Summit. While we have 48 users, the vast majority are internal staff, which are supplemented by a few beta users from the external community. The current breakdown is 41 internal accounts (staff, demonstrations, test) and 7 user accounts from 4 institutions.

We are making a special effort to ensure the system is providing relevant and useful data to the membership. We will have a continuing goal each quarter of reaching out to the membership to get them in to the system. We will further monitor the usage of the system and when warranted provide additional outreach and materials to sites that could be getting more out of the system. We must ensure that the system is relevant to the membership and provides them the data they need to manage their services. If we're not doing that then we need to modify our planning so we soon are.





Operational Status

The last quarter has seen two incidents of firewall scripting errors. Two different upgrades have resulted in a script change that leaves the internal server firewall disabled. We've addressed this with the developers and added specific monitoring to the system to alert us if it reoccurs and to enable the firewall again , inside of 1 minute.

This service is the first in Internet2 to use a provisioning management system. It's based around a workflow management tool and guides the staff through the steps in provisioning a new user, helping them with the required tasks, providing relevant documentation, and so on. It will provide reports on overall provisioning usage (how many users were provisioned) but also on how much time was spent in each step of the process, allowing us to identify and improve on our process.

Next Quarters Goals

- We would like to develop a strong sense of community around the service. The goal would be to encourage and sustain behavior such as users sharing queries and so on. To this end we want to develop a robust set of written documentation, online webinars, and video tutorials to help lead a mailing-list sort of conversation around how various sites are using the system.
- The application has the ability to track, hourly, top talkers by full IP address and destination. This is currently disabled. In the next four months we need to sort out the legal landscape around this feature and determine if we can enable that functionality while still providing reasonable privacy protections.
- We would like to add users from 32 institutions to the system.
- While the primary focus is on the membership, we would also like to ensure that the internal staff has the ability to take advantage of the system. We will be conducting an internal training session and working with the various Internet2 divisions to develop 4 use-cases around management/planning of the networks growth and usage.
- The system currently only has the TR-CPS and R&E routers configured. We would like to add the AL2S network devices, assuming sFlow support for the MX960 and MLX-16 arrives.
- We would like to extend the system to monitor MANlan, WIX, and Singapore via SFlow.
- Operationally, we would like to become more rigorous in how we manage the system. We would like to begin to perform routine capacity planning on the service, as well as fully document our alarming and emergency change process.

Timeline

10/4/13	Deepfield Products Ordered
1/8/14	Flow now pointed at the production server.
1/21/14	Experimental servers turned off.
1/22/14	Shib logins now working.
2/10/14	Firewall issues encountered and monitored.
3/10/14	Beta users: BU, OAR, MCNC
4/1/14	Software Update