from Customer Programs8 to Everyone:

Welcome to CA Office Hours for Network Flow Analysis. We will get started in about 10 minutes..

from Customer Programs8 to Everyone:

We will get started in 5 minutes. Please review the material on the slide ... thank you!

from Thiagarajah Ruben to Everyone:

What is the Number to call

from Customer Programs8 to Everyone:

@Thiagarajah: hello! there is no number to call - this is a webex chat ! :)

from Customer Programs8 to Everyone:

OK. We are ready to go! Hello Everyone! Welcome to CA Office Hours for Network Flow Analysis!

from Customer Programs8 to Everyone:

You can use the chat feature to start asking your questions. Who will be first ?

from Customer Programs8 to Everyone:

We have support engineers ready to talk to you. To ask a question just go to the chat feature, type in your question and click send...

from Barry Cole to Everyone:

Will a Flow Cloner be developed for Linux?

from stephen sheldon to Everyone:

Hello. I have a question about the flow packet cloner, I've installed it on a harvester and I see the exe and config file but can't find details on what to do with it beyond that. Simply running the exe just ends it right away. Does something else need to be done?

from Barry Cole to Everyone:

Any best practices for using Flow Forensics reports?

from Christopher Walsh to Everyone:

@stephen I wrote up a tech tip about flow cloning setup for 9.1.x and newer
https://communities.ca.com/docs/DOC-231149634

from Christopher Walsh to Everyone:

@stephen the NFA admin guide also covers the setup

from Martin Kowalewski to Everyone:

@Barry : No plan currently to add support for Linux. We are looking at adding Flow Cloner as a separate executable and operate as a standalone appliance to be a central point for netflow and then pass that to the appropriate harvesters.

from stephen sheldon to Everyone:

Ahhh, didn't see that it had a service, missed that part. Perfect! Thanks Chris!

from Amit Khandelwal to Everyone:

let me start .. how can we use netflow to monitor citrix xenapp environment

from Christopher Walsh to Everyone:

@Barry we recommend running the Flow Forensics reports for less than 4 hours and try to narrow it down a specific device, subnet etc instead of reporting on all. If you happen to ever see a Flow Forensics report get stuck in a 'Queued' state you can recycle the NetQos ReporterAnalyzer Report service on the NFA console server and it should get the report out of being 'queued'

from Ray Carter to Everyone:

Are there any best practices for interface aggregations?

from Barry Cole to Everyone:

@Christopher Thanks. I am currently running 2.2.3. Is there a good document on how to upgrade to the most recent iteration (2.4?)

from Ray Carter to Everyone:

Is there a knowledge doc on how one might want monitor MS Exchange traffic?

from Martin Kowalewski to Everyone:

@Barry: I would recommend that you follow the release notes and upgrade guide for CAPC for the steps and process to get to 2.4.

from Christopher Walsh to Everyone:

@amit if Xenapp uses a standard port number you can monitor the protocol based on that port number, or if your Cisco device supports NBAR2 you can use NFA 9.2's new NBAR2 reporting feature

from Lekshmi to Everyone:

Does NFA support Netstream?

from Christopher Walsh to Everyone:

@ray you can use the new NBAR2 feature in NFA 9.2 there are more details in the NFA admin guide, but I did post a tech tip about how to verify the NBAR2 data coming in using wireshark https://communities.ca.com/docs/DOC-231149649

from Amit Khandelwal to Everyone:

i am using a virtual switch on an esx

from sarah mulvihill to Everyone:

what's best practice when a router is upgraded to ensure the interface historical data is merged with new? We have had instances where we have to delete router and start over losing historical data.

from Christopher Walsh to Everyone:

@Lekshmi if the NetStream sends the standard fields we require for NetFlow traffic then yes, the required NetFlow fields and how to verify them are posted in the tech tip https://communities.ca.com/docs/DOC-231149629

from Barry Cole to Everyone:

Can Harvester and Performance Center be installed on the same VM?

from Martin Kowalewski to Everyone:

@Amit: You can export netflow from Vmware ESXi 5.5 which we do support, so we will see all protocols and applications that are coming through the Vswitch. However, what it will not give you is specific response times of those applications.

from Amit Khandelwal to Everyone:

dont suppse @barry

from Manuel Preclaro to Everyone:

@ray We have no doc for best practice other than the Hot to in our Admin guide.

from Amit Khandelwal to Everyone:

i am already collecting data from virtual switch and also instrumented ADA

from Christopher Walsh to Everyone:

@sarah there have been some improvements to the mapping process in 9.2.1 which is due out soon which would help the scenario you laid out. In the current versions you would have to do a merge on the interfaces

from Martin Kowalewski to Everyone:

@Barry: Can you clarify Performance Center as NPC or CAPC?

from Manuel Preclaro to Everyone:

@Barry Technically yes but we highly recommend installing NPC on it's own VM.

from jacquie to Everyone:

how do i export all the devices out of our current instance and their respective groups?

from Barry Cole to Everyone:

@Manuel: CAPC

from Amit Khandelwal to Everyone:

CA PC requires linux and can harvestor be installed on linux

from Lekshmi to Everyone:

Do we have config for netstream implementation the way we have for Netflow?

from Christopher Walsh to Everyone:

@jacquie currently there is no way export devices and their respective groups wihtout a full database backup and restore

from Barry Cole to Everyone:

@Amit: I have Harvester running on RHEL 5.6

from Manuel Preclaro to Everyone:

@Barry The same applies for CAPC

from stephen sheldon to Everyone:

I was told by support (case 21786271 01) that the Netflow sent by VMware 5.5 (v10 - IPFIX) is not supported. Just now though its said that it was. Can you clarify that?

from jacquie to Everyone:

i need to do a database backup/restore to get a list of the devices and their groups? no commands that I can run to do this?

from Manuel Preclaro to Everyone:

@Amit Yes the Harvester can be installed on linux

from Amit Khandelwal to Everyone:

thanks @ barry .. i thought it wasnt

from jacquie to Everyone:

i need weekly status checks to compare with whats configured within our flow replicator

from Christopher Walsh to Everyone:

@lekshmi unfortunately we do not have configurations for each device, it is usually best to contact the vendor directly for NetFlow configuration. We have some examples gathered by the user community published here https://communities.ca.com/docs/DOC-1061 however Netstream is not on that document

from Martin Kowalewski to Everyone:

@Stephen: ESXi IPFIX should work, we will need to work directly with you on that issue.

from Amit Khandelwal to Everyone:

@martin & barry . i have implemented that in LOD

from Christopher Walsh to Everyone:

@jacquie the exporting of devices would be the easy part via mysql however the group association can be tough to keep up aligned. This would be a good Idea you can raise as an enhancement on the User Communities

from Lekshmi to Everyone:

Should we integrate NFA with Spectrum or SOI? Which one is best practice

from Christopher Walsh to Everyone:

@Stephen we would likely need to review a PCAP again on that issue in support to see what may be different in your ESX netflow, there may be a missing NetFlow field

from Amit Khandelwal to Everyone:

@barry link for vmware which says ipfix is supported
https://www.vmware.com/files/pdf/techpaper/Whats-New-VMware-vSphere-51-Network-Technical-Whitepaper.pdf

from Christopher Walsh to Everyone:

@Lekshmi we would recommend Spectrum

from Juan Jaramillo to Everyone:

can be made as custom views and do?

from Amit Khandelwal to Everyone:

so when we monitor esxi virtual switch , all i am going to get is protocol level breakup and not response time of applications .. is that understanding right

from Martin Kowalewski to Everyone:

@Amit: That is correct, no response times. We would leverage ADA Virtual Collector for response times of the applications running on the Virtual Machines.

from Christopher Walsh to Everyone:

@juan can you clarify? Are you looking for Custom Views in NFA? We do not have too many options for Custom Views in NFA, but we do have Custom Reports, Flow Forensics Reports, and Analysis reports which allow you to create a variety of reports which most can be scheduled, exported, and emailed

from Barry Cole to Everyone:

How does Spectrum tie in to Custom Reports, Flow Forensics Reports, and Analysis reports? i.e What would the Global Collection's composition be in order to leverage it in reporting?

from Juan Jaramillo to Everyone:

@Christopher: Please you can send the link to the reports documuetnacion NFA offers?

from Christopher Walsh to Everyone:

@juan the full NFA 9.2 bookshelf is available here https://support.ca.com/cadocs/0/CA%20Network%20Flow%20Analysis%209%202%200-ENU/Bookshelf.html

the Admin and User guides would describe all of our report types

from Barry Cole to Everyone:

Asked differently, has anyone used Spectrum in NFA reporting?

from Martin Kowalewski to Everyone:

@Barry: The Spectrum integration does not leverage the reporting component, but operationally we would send analysis traps from NFA to Spectrum then from the alarm you could drill back to NPC/NFA in context for further analysis.

from Juan Jaramillo to Everyone:

Is possible to generate alerts(spectrum) when an interface discovered in NFA is found flow off?

from Christopher Walsh to Everyone:

@juan we don't send traps from NFA for when an interface is not sending flow. The admin guide I linked you before covers what we can send trap alerts on, mostly it is based on an interface going over a certain threshold

from Christopher Walsh to Everyone:

@jaun a great idea that can be submitted on the user communities

from Christopher Walsh to Everyone:

https://communities.ca.com/community/ca-infrastructure-management/overview

from Customer Programs8 to Everyone:

We have 20 more minutes for this Office Hours session. The questions coming in are great... thank you for sending them in... Are there any more questions we can assist with?

from Lekshmi to Everyone:

Best practices for using NFA in brief if anyone could suggest

from Juan Jaramillo to Everyone:

what kind of report I can get the interfaces that are reporting flow to NFA but not yet activated?

from Barry Cole to Everyone:

@Lekshmi: We are planning on using the NFA to run a monthly Capacity Planning report with just a single click.

from Christopher Walsh to Everyone:

@lekshmi can you be a bit more specific. I would start by getting links to the bookshelf for NFA and referencing the documnetation, there is some great resources in there.

from Lekshmi to Everyone:

It was my client requirement to suggest best practices on using NFA..

from Lekshmi to Everyone:

So if you could let me know in some pointers on how NFA should be used for optimal use of network monitoring

from Christopher Walsh to Everyone:

@lekshmi Here is the link to the NFA documentation for 9.2
https://support.ca.com/cadocs/0/CA%20Network%20Flow%20Analysis%209%202%200-ENU/Bookshelf.html

from Ray Carter to Everyone:

To add to Lekshmi's question - so netflow is being collected... what are 1 or 2 other next steps that most customers do to leverage data? Aggregation, Reporting, etc.? What's some of the capabilities customers' most leverage?

from Lekshmi to Everyone:

Ok Thank you..Any suggestions from previous experience

from Lekshmi to Everyone:

They are new to tool..so we need to suggest them..

from Christopher Walsh to Everyone:

@juan there is no report currently to report on what is enabled but not receving data. Another great idea for the user communities. MySql could be leveraged manually to get an idea of what is enabled but has not seen a flow in a certain period of time. If you want to open a support issue we may be able to help out with that.

from Manuel Preclaro to Everyone:

@juan NFA doesn't have any reports that will list the inactive interfaces. We can probably create a mysql quesy for you if you open an issue with support.

from Christopher Walsh to Everyone:

@ray @lekshmi many customers will leavel the Auto Enable interfaces turned off as to not license too many interfaces all at once. As far as other use cases you may want to post in the user communities to see how other users manage their environments.

from Lekshmi to Everyone:

Sure..Thanks

from Amit Khandelwal to Everyone:

can we also have a document highlighting the metrics/parameters which we can pull from Vmware logical switch

from Christopher Walsh to Everyone:

@amit the main fields we use in NetFlow are: 1 - IN_BYTES or 85 – IN_PERMANENT_BYTES (NFA Only)
4 - PROTOCOL
7 - L4_SRC_PORT
8 - IPV4_SRC_ADDR
10 - INPUT_SNMP
11 - L4_DST_PORT
12 - IPV4_DST_ADDR
14 - OUTPUT_SNMP

from Christopher Walsh to Everyone:

which translate to Source IP address
Ø Destination IP address
Ø Source port
Ø Destination port Protocol type
Ø Class of service
Ø Input logical interface (ifIndex)

from Christopher Walsh to Everyone:

There are some additional fields you may see in Flow Forensics reports

from Customer Programs8 to Everyone:

Hello Everyone. we have 5 more minutes left for final questions...

from Christopher Walsh to Everyone:

@amit as well as NBAR2 fields which are now support in NFA 9.2, however I am not certain if VMSwitch uses NBAR2 at this time

from Juan Jaramillo to Everyone:

Thank you very much, hope to have more time to share future questions about NFA

from Christopher Walsh to Everyone:

Thanks @jaun feel free to post in the User Communities and we will try to answer questions there as well

from Lekshmi to Everyone:

Thanks for the Assistance

from Customer Programs8 to Everyone:

Thank you for joining todays' Office Hours for NFA

from Customer Programs8 to Everyone:

We will be posting the transcripts from today's session to the IM Community.

from Customer Programs8 to Everyone:

https://communities.ca.com/community/ca-infrastructure-management

from Customer Programs8 to Everyone:

Thank you very much for attending! Have a wonderful day!